Linee Guida

Linee guida 3/2022

Modelli di progettazione ingannevoli nelle interfacce delle piattaforme di social media:

come riconoscerli ed evitarli

Versione 2.0

Adottate il 14 febbraio 2023

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Cronologia delle versioni

Versione 2.0	14 febbraio 2023	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	14 marzo 2022	Adozione delle linee guida per la consultazione pubblica

SCHEDA DI SINTESI

Le presenti linee guida offrono raccomandazioni pratiche ai fornitori di social media in qualità di titolari del trattamento sui social media, ai progettisti e agli utenti delle piattaforme di social media su come valutare ed evitare i cosiddetti "modelli di progettazione ingannevoli" nelle interfacce dei social media, che violano il regolamento generale sulla protezione dei dati (GDPR). A tal fine l'EDPB raccomanda ai titolari del trattamento di avvalersi di gruppi interdisciplinari, composti, tra gli altri, da progettisti, responsabili della protezione dei dati e decisori. Si richiama l'attenzione sul fatto che l'elenco dei modelli di progettazione ingannevoli e delle migliori prassi, così come i casi d'uso non sono esaustivi. La competenza e la responsabilità di garantire la conformità delle piattaforme al GDPR restano in capo ai fornitori di social media.

Modelli di progettazione ingannevoli nelle interfacce delle piattaforme di social media

Nel contesto delle presenti linee guida, con "modelli di progettazione ingannevoli" si intendono interfacce e percorsi utente applicati su piattaforme di social media che tentano di influenzare l'utente affinché prenda, riguardo al trattamento dei propri dati personali, decisioni inconsapevoli, non volute e potenzialmente dannose, spesso contrarie ai propri interessi ma favorevoli a quelli delle piattaforme di social media. I modelli di progettazione ingannevoli mirano a influenzare il comportamento degli utenti e possono ostacolare la loro capacità di proteggere efficacemente i propri dati personali e di compiere scelte consapevoli. Le autorità preposte alla protezione dei dati hanno il compito di sanzionare l'uso di modelli di progettazione ingannevoli in caso di violazione delle prescrizioni del GDPR. I modelli di progettazione ingannevoli esaminati nelle presenti linee guida possono essere suddivisi nelle categorie elencate di seguito.

- ***Overloading*** (sovraccarico): gli utenti si trovano di fronte a una moltitudine/grande quantità di richieste, informazioni, opzioni o possibilità finalizzate a spingerli a condividere un maggior numero di dati oppure a consentire involontariamente un trattamento dei dati personali contrastante con le aspettative dell'interessato.
  Rientrano in questa categoria i seguenti tre tipi di modelli di progettazione ingannevoli: ***Continuous prompting*** (sollecitazione continua), ***Privacy Maze*** (privacy intricata) e ***Too Many Options*** (troppe opzioni);

- ***Skipping*** (saltare): le interfacce o i percorsi utente sono progettati in modo tale che gli utenti dimentichino completamente o in parte gli aspetti legati alla protezione dei propri dati o non vi riflettano.
  Rientrano in questa categoria i seguenti due tipi di modelli di progettazione ingannevoli: ***Deceptive Snugness*** (comodità ingannevole) e ***Look over there*** (diversivo);

- ***Stirring*** (infondere agitazione): le scelte degli utenti sono influenzate facendo leva sulle emozioni degli utenti o usando sollecitazioni visive.
  Rientrano in questa categoria i seguenti due tipi di modelli di progettazione ingannevoli: ***Emotional Steering*** (stimolazione emotiva) e ***Hidden in plain sight*** (poca visibilità);

- ***Obstructing*** (creazione di ostacoli): consiste nell'ostacolare o bloccare gli utenti nel processo di acquisizione delle informazioni sull'uso dei propri dati o di gestione degli stessi rendendo difficile o impossibile la sua realizzazione.
  Rientrano in questa categoria i seguenti tre tipi di modelli di progettazione ingannevoli: ***Dead end*** (punto morto), ***Longer than necessary*** (allungare più del necessario) e ***Misleading action*** (azione ingannevole);

- ***Fickle*** (ambiguità): a causa di un'interfaccia progettata in modo incoerente o poco chiaro, gli utenti hanno difficoltà a orientarsi nei diversi strumenti di controllo della protezione dei dati e a comprendere quali siano le finalità del trattamento.
  Rientrano in questa categoria i seguenti quattro tipi di modelli di progettazione ingannevoli: ***Lacking hierarchy*** (mancanza di gerarchia), ***Decontextualising*** (decontestualizzazione), ***Inconsistent Interface*** (interfaccia incoerente) e ***Language Discontinuity*** (discontinuità linguistica);

- ***Left in the dark*** (lasciare all'oscuro): l'interfaccia è progettata in modo da nascondere le informazioni o gli strumenti di controllo della protezione dei dati o in modo da lasciare gli utenti nell'incertezza sulle modalità di trattamento dei loro dati e sul tipo di controllo che potrebbero avere su di essi per quanto riguarda l'esercizio dei propri diritti.
  Rientrano in questa categoria i seguenti due tipi di modelli di progettazione ingannevoli: ***Conflicting information*** (informazioni contrastanti) e ***Ambiguous wording or information*** (formulazioni o informazioni ambigue).

Disposizioni del GDPR pertinenti ai fini delle valutazioni dei modelli di progettazione ingannevoli

Per quanto riguarda il rispetto delle norme in materia di protezione dei dati da parte delle interfacce utente delle applicazioni online nel settore dei social media, i principi di protezione dei dati applicabili sono stabiliti all'articolo 5 GDPR. Il principio di trattamento corretto di cui all'articolo 5, paragrafo 1, lettera a), GDPR funge da punto di partenza per valutare se un modello di progettazione si configuri effettivamente come "modello di progettazione ingannevole". Altri principi importanti ai fini della valutazione sono quelli della trasparenza, della minimizzazione dei dati e della responsabilizzazione ai sensi dell'articolo 5, paragrafo 1, lettere a) e c), e dell'articolo 5, paragrafo 2, GDPR, nonché, in alcuni casi, quello della limitazione della finalità ai sensi dell'articolo 5, paragrafo 1, lettera b), GDPR. In altri casi, la valutazione sotto il profilo giuridico si basa anche sulle condizioni del consenso di cui all'articolo 4, punto 11), e all'articolo 7 GDPR o su altri obblighi specifici, come quelli di cui all'articolo 12 GDPR. È evidente che, nel contesto dei diritti degli interessati, occorre tenere conto anche del terzo capo del GDPR. Sono infine d'importanza fondamentale i requisiti relativi alla protezione dei dati fin dalla progettazione e per impostazione predefinita ai sensi dell'articolo 25 GDPR, in quanto la loro applicazione prima di avviare una progettazione di interfaccia aiuterebbe i fornitori di social media a evitare modelli di progettazione ingannevoli.

Esempi di modelli di progettazione ingannevoli in casi d'uso relativi al ciclo di vita di un account di social media

Le disposizioni del GDPR si applicano all'intero corso del trattamento dei dati personali nell'ambito della gestione delle piattaforme di social media, ossia all'intero ciclo di vita di un account utente. L'EDPB fornisce esempi concreti di tipi di modelli di progettazione ingannevoli per i seguenti diversi

casi d'uso nel corso del ciclo di vita di un account utente: l'iscrizione, ossia il processo di registrazione; i casi d'uso relativi alle informazioni, riguardanti l'informativa sulla privacy, la contitolarità del trattamento e le comunicazioni relative a violazioni dei dati; la gestione del consenso e della protezione dei dati; l'esercizio dei diritti degli interessati durante l'utilizzo dei social media; e infine la chiusura di un account sui social media. I collegamenti con le disposizioni del GDPR sono spiegati in due modi: in primo luogo, ciascun caso d'uso precisa in modo più dettagliato quali delle citate disposizioni del GDPR sono particolarmente pertinenti. In secondo luogo, i paragrafi relativi agli esempi di modelli di progettazione ingannevoli spiegano in che modo essi violano il GDPR.

Raccomandazioni sulle migliori prassi

Nelle linee guida, oltre agli esempi di modelli di progettazione ingannevoli, alla fine di ciascun caso d'uso nonché nell'allegato II sono illustrate le migliori prassi, che contengono raccomandazioni specifiche per la progettazione di interfacce utente che facilitino l'efficace attuazione del GDPR.

Lista di controllo delle categorie di modelli di progettazione ingannevoli

Nell'allegato I delle presenti linee guida è riportata una lista di controllo delle categorie di modelli di progettazione ingannevoli, che fornisce una panoramica di dette categorie e dei tipi di modelli di progettazione ingannevoli, insieme a un elenco degli esempi per ciascun modello che sono menzionati nei casi d'uso. La lista di controllo potrebbe risultare utile per esplorare il contenuto delle presenti linee guida.

Indice

Il Comitato europeo per la protezione dei dati

visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito "GDPR"),

visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37, modificati dalla decisione del Comitato misto SEE n. 154/2018 del 6 luglio 2018[1],

visti gli articoli 12 e 22 del proprio regolamento interno,

HA ADOTTATO LE SEGUENTI LINEE GUIDA

1 AMBITO DI APPLICAZIONE

1. L'obiettivo delle presenti linee guida è fornire raccomandazioni e orientamenti per la progettazione delle interfacce delle piattaforme di social media. Ai fini delle presenti linee guida, con "social media" si intendono piattaforme online che consentono lo sviluppo di reti e di comunità di utenti, tra i quali vengono condivisi contenuti e informazioni[2]. Le linee guida possono essere utilizzate nella fase di ideazione di un'interfaccia utente, per evitare fin dall'inizio la realizzazione di modelli di progettazione ingannevoli[3], o su un servizio esistente, per valutare la conformità della sua interfaccia. Si rivolgono ai fornitori di social media in qualità di titolari del trattamento sui social media, a cui incombe la responsabilità della progettazione e della gestione delle piattaforme di social media. A tale riguardo le linee guida intendono richiamare l'attenzione sugli obblighi derivanti dal GDPR, con particolare riferimento ai principi di liceità, correttezza, trasparenza, limitazione delle finalità e minimizzazione dei dati nella progettazione delle interfacce utente e nella presentazione dei contenuti dei relativi servizi web e applicazioni. Detti principi devono essere applicati in modo sostanziale e, da un punto di vista tecnico, costituiscono i requisiti per la progettazione di software e servizi, comprese le interfacce utente. Le presenti linee guida esaminano in modo approfondito l'applicazione delle disposizioni del GDPR alle interfacce utente e alla presentazione dei contenuti e chiariscono ciò che dovrebbe essere considerato un "modello di progettazione ingannevole", ossia una modalità di progettazione e presentazione dei contenuti che viola in maniera sostanziale tali requisiti pur facendo credere di rispettarli formalmente. Le presenti linee guida possono inoltre sensibilizzare maggiormente gli utenti in merito ai propri diritti e ai rischi che potrebbero derivare dalla condivisione di una quantità eccessiva di dati o dalla condivisione dei propri dati senza alcun controllo. Esse mirano altresì a educare gli utenti a riconoscere i "modelli di progettazione ingannevoli" (quali definiti in appresso) e a sapere come affrontarli per proteggere la propria vita privata in modo consapevole. Nell'ambito dell'analisi, il ciclo

[1] Nel presente documento con il termine "Stati membri" si intendono gli "Stati membri del SEE".

[2] Definizione identica a quella contenuta nelle linee guida 8/2020 dell'EDPB sul *targeting* degli utenti di social media, punto 1, cfr. nota a piè di pagina 1 per una descrizione più dettagliata; disponibile all'indirizzo: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_it_0.pdf.

[3] Per la versione 2.0 delle presenti linee guida, l'EDPB utilizza il termine più inclusivo e descrittivo "modello di progettazione ingannevole" anziché "modello oscuro".

di vita di un account sui social media è stato esaminato sulla base di cinque casi d'uso: "Apertura di un account sui social media" (caso d'uso n. 1), "Stare in modo informato sui social media" (caso d'uso n. 2), "Rimanere protetti sui social media" (caso d'uso n. 3), "Rimanere dal lato dei diritti sui social media: i diritti dell'interessato "(caso d'uso n. 4) e "Addio e arrivederci: abbandonare un account sui social media "(caso d'uso n. 5).

2. Nelle presenti linee guida il termine "interfaccia utente" indica i mezzi che consentono alle persone di interagire con le piattaforme di social media. Il documento si concentra sulle interfacce utente grafiche (utilizzate ad esempio per le interfacce per computer e smartphone), ma alcune delle osservazioni formulate possono applicarsi anche alle interfacce con controllo vocale (utilizzate ad esempio per gli altoparlanti intelligenti) o alle interfacce basate sui gesti (utilizzate ad esempio in ambienti di realtà virtuale). Il termine "percorso utente" indica la serie di azioni o passaggi che l'utente deve compiere per raggiungere il proprio obiettivo che, sui social network, può riguardare aspetti quali la navigazione sul proprio feed, la condivisione di un post, la definizione delle preferenze ecc. Il termine "esperienza utente" indica l'esperienza complessiva degli utenti con le piattaforme di social media, che comprende l'utilità percepita, la facilità d'uso e l'efficienza dell'interazione con la piattaforma. Nell'ultimo decennio la progettazione delle interfacce utente e quella delle esperienze utente hanno registrato una continua evoluzione. Più di recente sono state privilegiate interazioni ed esperienze utente ubiquitarie, personalizzate e cosiddette "senza soluzione di continuità": l'interfaccia perfetta dovrebbe essere altamente personalizzata, di facile utilizzo e multimodale[4]. Benché da un lato possano migliorare la facilità di utilizzo dei servizi digitali, dall'altro tali tendenze possono essere utilizzate in modo da incentivare principalmente comportamenti degli utenti contrari allo spirito del GDPR[5]. Si tratta di un aspetto particolarmente pertinente nel contesto dell'economia dell'attenzione, in cui l'attenzione dell'utente è considerata un bene. In tali circostanze, può accadere che i limiti di quanto legalmente consentito a norma del GDPR siano oltrepassati. I casi in cui la progettazione dell'interfaccia e la progettazione dell'esperienza utente conducono a tali circostanze sono descritti di seguito come "modelli di progettazione ingannevoli"

3. Nel contesto delle presenti linee guida, con "modelli di progettazione ingannevoli" si intendono interfacce e percorsi utente applicati su piattaforme di social media volti a influenzare l'utente affinché prenda, riguardo al trattamento dei propri dati personali, decisioni inconsapevoli, rispettivamente non volute e/o potenzialmente dannose, spesso contrarie ai propri interessi ma favorevoli a quelli delle piattaforme di social media. I modelli di progettazione ingannevoli mirano a influenzare i comportamenti dell'utente, generalmente basandosi su *bias* cognitivi, e possono ostacolare la sua capacità di proteggere efficacemente i propri dati personali e compiere scelte consapevoli[6], ad esempio mettendolo nelle condizioni di non poter prestare un consenso informato ed espresso liberamente[7]. A tal fine possono essere sfruttati diversi aspetti della progettazione, come la scelta del colore dell'interfaccia e la collocazione dei contenuti. Al contrario, fornendo incentivi e progettazioni di facile utilizzo, si può agevolare l'applicazione delle norme in materia di protezione dei dati.

[4] Per maggiori dettagli cfr. CNIL, relazione sulla PI n. 6: *Shaping Choices in the Digital World*, 2019. p. 9 https://www.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[5] CNIL, *Shaping Choices in the Digital World*, 2019, pag. 10.

[6] CNIL, *Shaping Choices in the Digital World*, 2019, pag.27.

[7] Cfr. Consiglio dei consumatori norvegese, *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*, pag. 10 https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf, e anche CNIL, *Shaping Choices in the Digital World*, pagg. 30 e 31.

4. I modelli di progettazione ingannevoli non comportano necessariamente soltanto la violazione delle norme in materia di protezione dei dati, ma possono, ad esempio, violare anche le norme in materia di protezione dei consumatori. I confini tra le violazioni sanzionabili dalle autorità di protezione dei dati e quelle sanzionabili dalle autorità nazionali preposte alla tutela dei consumatori, alla concorrenza o ad altre autorità possono sovrapporsi[8]. A norma del GDPR, le autorità di protezione dei dati sono competenti a sanzionare l'uso di modelli di progettazione ingannevoli se questi violano di fatto le norme in materia di protezione dei dati e, di conseguenza, il GDPR. Le violazioni delle disposizioni del GDPR devono essere valutate caso per caso. Le presenti linee guida riguardano soltanto i modelli di progettazione ingannevoli che potrebbero rientrare in tale mandato normativo. Per questo motivo, oltre agli esempi di modelli di progettazione ingannevoli, le linee guida presentano anche le migliori prassi che possono essere utilizzate per progettare interfacce utente che facilitino l'efficace attuazione del GDPR. Tali migliori prassi possono rappresentare un primo passo verso un modo standardizzato per consentire agli utenti di controllare efficacemente i propri dati e di esercitare i propri diritti.

5. I modelli di progettazione ingannevoli[9] trattati nelle presenti linee guida derivano da un'analisi interdisciplinare delle interfacce esistenti e possono essere suddivisi nelle categorie elencate di seguito.

Overloading (sovraccarico): gli utenti si trovano di fronte a una moltitudine/una grande quantità di richieste, informazioni, opzioni o possibilità finalizzate a spingerli a condividere un maggior numero di dati oppure a consentire involontariamente un trattamento dei dati personali contrastante con le aspettative dell'interessato.

Skipping (saltare): le interfacce o i percorsi utente sono progettati in modo tale che gli utenti dimentichino del tutto o in parte gli aspetti legati alla protezione dei dati o non vi riflettano.

Stirring (infondere agitazione): le scelte degli utenti sono influenzate facendo leva sulle loro emozioni o utilizzando sollecitazioni visive.

Obstructing (creazione di ostacoli): ostacolare o bloccare gli utenti nel processo di acquisizione delle informazioni sull'uso dei propri dati o nella gestione dei propri dati rendendo difficile o impossibile la sua realizzazione.

Fickle (ambiguità): gli utenti hanno difficoltà a orientarsi nei diversi strumenti di controllo della protezione dei dati e a comprendere quali siano le finalità del trattamento a causa di un'interfaccia progettata in modo incoerente o poco chiaro.

Left in the dark (lasciare all'oscuro): l'interfaccia è progettata in modo da nascondere le informazioni o gli strumenti di controllo della protezione dei dati o in modo da lasciare gli utenti nell'incertezza sulle

[8] A tale riguardo, l'articolo 25, paragrafo 2, del regolamento (UE) 2022/2065, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali), chiarisce che il divieto di progettare interfacce online in modo ingannevole o manipolatorio di cui all'articolo 25, paragrafo 1, del medesimo regolamento, non si applica alle pratiche contemplate dalla direttiva 2005/29/CE (direttiva relativa alle pratiche commerciali sleali tra imprese e consumatori, UCPD) o dal GDPR. Inoltre la comunicazione della Commissione europea (2021/C 526/01), nella sezione 4.2.7, fornisce orientamenti sull'interpretazione e l'applicazione della direttiva relativa alle pratiche commerciali sleali, anche per quanto riguarda i "modelli oscuri".

[9] Le categorie di modelli di progettazione ingannevoli e i tipi di modelli di progettazione ingannevoli all'interno di tali categorie saranno visualizzati ***in grassetto e in corsivo*** nel testo delle linee guida. Nell'allegato è fornita una panoramica dettagliata.

modalità di trattamento dei loro dati e sul tipo di controllo che potrebbero avere su di essi per quanto riguarda l'esercizio dei loro diritti.

6. Oltre che raggruppati in queste categorie sulla base dei loro effetti sul comportamento degli utenti, tali modelli di progettazione ingannevoli possono anche essere suddivisi in modelli basati sui contenuti e modelli basati sull'interfaccia, al fine di affrontare in modo più specifico aspetti dell'interfaccia utente o del percorso utente. I modelli basati sui contenuti si riferiscono al contenuto effettivo e quindi anche alla formulazione e al contesto delle frasi e degli elementi informativi. Tuttavia vi sono anche componenti che hanno un'influenza diretta sulla percezione di tali fattori. Questi modelli basati sull'interfaccia sono legati alle modalità di visualizzazione dei contenuti, di navigazione o di interazione con essi.

7. È essenziale tenere presente che i modelli di progettazione ingannevoli sono motivo di ulteriori preoccupazioni per quanto riguarda il potenziale impatto sui minori[10] che si registrano sulla piattaforma di social media, come pure su altri gruppi vulnerabili quali gli anziani, le persone con disabilità visive o che non dispongono dello stesso livello di alfabetizzazione digitale degli altri. I gruppi vulnerabili, come gli utenti anziani, spesso non solo sono meno in grado di individuare pratiche di progettazione manipolatorie, ma sono anche meno consapevoli del fatto che il loro comportamento digitale è influenzabile. Il GDPR prevede garanzie supplementari quando il trattamento riguarda i dati personali dei minori, in quanto questi ultimi possono essere meno consapevoli dei rischi e delle conseguenze riguardanti i loro diritti relativi al trattamento[11]. Il considerando 58 afferma esplicitamente che, quando il trattamento riguarda un minore, qualsiasi informazione dovrebbe essere fornita in un linguaggio semplice e chiaro che i minori possano capire. Inoltre il GDPR include esplicitamente il trattamento dei dati delle persone fisiche, in particolare dei minori, tra le situazioni in cui i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale[12].

8. Alla luce di quanto precede, dovrebbe essere chiaro che i modelli di progettazione ingannevoli non riguardano esclusivamente le piattaforme di social media. Nel corso della consultazione pubblica relativa alle presenti linee guida sono stati espressi pareri netti su tale questione. Le interfacce sono presenti in molti altri casi in cui gli utenti interagiscono con prodotti e servizi basati su operazioni di trattamento dei dati o ad esse collegati. Può trattarsi di siti web o di cookie banner[13], negozi online, videogiochi, applicazioni mobili e micropagamenti ecc. Sebbene i modelli di progettazione ingannevoli descritti di seguito non siano sempre presenti esattamente nella stessa forma, le loro variazioni possono comunque violare i diritti degli interessati o dei consumatori. Tuttavia le presenti linee guida sono dedicate esclusivamente ai modelli di progettazione ingannevoli nelle piattaforme di social

[10] Cfr. anche considerando 81, quarta frase, del regolamento (UE) 2022/2065 (regolamento sui servizi digitali).
[11] GDPR, considerando 38.
[12] GDPR, considerando 75; cfr. anche le linee guida 8/2020 dell'EDPB sul *targeting* degli utenti di social media, punto 16 https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_it.pdf.
[13] Sollecitata da una serie di reclami ricevuti da NOYB, una task force dell'EDPB ha proceduto a uno scambio di opinioni su una serie di elementi di progettazione di cookie banner. Il denominatore comune concordato dalle autorità di controllo nella loro interpretazione del quadro giuridico articolato su più livelli applicabile è stato sintetizzato in una relazione del lavoro svolto dalla task force Cookie Banner del 17 gennaio 2023, disponibile all'indirizzo https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf.

media, in quanto l'influenza di tali piattaforme sulla vita quotidiana delle persone e delle nazioni cresce costantemente, come è stato chiarito nei precedenti documenti dell'EDPB[14].

2 PRINCIPI APPLICABILI — COSA VA TENUTO PRESENTE?

9. Per quanto riguarda il rispetto delle norme in materia di protezione dei dati da parte delle interfacce utente delle applicazioni online nel settore dei social media, i principi di protezione dei dati applicabili sono stabiliti all'articolo 5 GDPR. Il principio del trattamento corretto di cui all'articolo 5, paragrafo 1, lettera a), GDPR è un punto di partenza per valutare l'esistenza di modelli di progettazione ingannevoli. Come già affermato dall'EDPB, la correttezza è un principio di natura trasversale secondo cui i dati personali non devono essere trattati in modo dannoso, discriminatorio, imprevisto o fuorviante per l'interessato[15]. Se l'interfaccia contiene informazioni insufficienti o fuorvianti per gli utenti e risponde alle caratteristiche dei modelli di progettazione ingannevoli, può configurarsi un trattamento non corretto. Il principio di correttezza ha una funzione trasversale e tutti i modelli di progettazione ingannevoli lo violerebbero, indipendentemente dal rispetto di altri principi di protezione dei dati.

10. Oltre a questa disposizione fondamentale riguardante la correttezza del trattamento, i principi di responsabilizzazione, trasparenza e l'obbligo di protezione dei dati fin dalla progettazione di cui all'articolo 25 GDPR sono pertinenti anche per quanto riguarda l'ambito della progettazione e i modelli di progettazione ingannevoli potrebbero violarli. Tuttavia è anche possibile che la valutazione sotto il profilo giuridico dei modelli di progettazione ingannevoli possa basarsi su elementi relativi a definizioni generali quali l'articolo 4, punto 11), GDPR contenente la definizione di consenso o su altri obblighi specifici di cui all'articolo 12 GDPR. L'articolo 12, paragrafo 1, prima frase, GDPR impone ai titolari del trattamento di adottare misure appropriate per fornire tutte le comunicazioni relative ai diritti dell'interessato e le informazioni in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Come emerge dal considerando 39, terza frase, relativa al principio di trasparenza, tale obbligo non è tuttavia limitato alle informative sulla protezione dei dati[16] o ai diritti degli interessati[17], ma si applica a qualsiasi informazione e comunicazione relativa al trattamento dei dati personali. Il considerando precisa inoltre, nella quinta frase, che le persone interessate dovrebbero essere sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento.

11. Per la progettazione delle interfacce utente delle applicazioni online, è altresì importante tenere conto del principio della limitazione delle finalità ai sensi dell'articolo 5, paragrafo 1, lettera b), GDPR, così come del principio della minimizzazione dei dati ai sensi dell'articolo 5, paragrafo 1, lettera c), GDPR. In ogni caso, per garantire il rispetto delle norme in materia di protezione dei dati, si consiglia ai titolari del trattamento di verificare il rispetto di tutti i principi di protezione dei dati ai sensi del GDPR.

---

[14] EDPS, *Linee guida 8/2020 sul targeting degli utenti dei social media*; EDPS, Dichiarazione 2/2019 sull'uso dei dati personali nel corso di campagne politiche https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-22019-use-personal-data-course-political_it.

[15] EDPB, *Linee guida 4/20219 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita*, versione 2.0, adottate il 20 ottobre 2020, pag. 16; https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_it.

[16] Aspetto trattato nella parte 3.2. — caso d'uso n. 2a delle presenti linee guida.

[17] Aspetto trattato nei casi d'uso nn. 4 e 5, ossia le parti 3.4 e 3.5 delle presenti linee guida.

2.1 Responsabilizzazione

12. Il principio di responsabilizzazione deve essere applicato nella progettazione di ogni interfaccia utente.

13. L'articolo 5, paragrafo 2, GDPR stabilisce che il titolare del trattamento è competente per il rispetto dei principi descritti all'articolo 5, paragrafo 1, del medesimo regolamento, ed è in grado di comprovarlo. Pertanto tale principio è strettamente collegato ai principi pertinenti di cui sopra. La responsabilizzazione può essere garantita da elementi che dimostrano la conformità al GDPR da parte del fornitore di social media. L'interfaccia utente e il percorso utente possono essere utilizzati come strumento di documentazione per dimostrare che, durante le loro azioni sulla piattaforma di social media, gli utenti hanno letto le informazioni sulla protezione dei dati e hanno tenuto conto delle stesse, hanno liberamente espresso il proprio consenso, hanno esercitato facilmente i propri diritti ecc. Per comprovare la conformità possono essere usati anche metodi qualitativi e quantitativi di ricerca sugli utenti, come i test A/B, il tracciamento oculare o le interviste di utenti. È importante osservare che tali metodi di ricerca spesso comportano anche il trattamento di dati personali, che pertanto deve essere conforme al GDPR. Se, ad esempio, gli utenti devono spuntare una casella o cliccare su una delle opzioni di protezione dei dati, le schermate delle interfacce possono servire a mostrare il percorso degli utenti attraverso le informazioni sulla protezione dei dati e a spiegare in che modo gli utenti stessi prendano una decisione informata. I risultati delle ricerche condotte sugli utenti effettuate sull'interfaccia in questione apporterebbero ulteriori elementi utili a spiegare il motivo per cui l'interfaccia è ottimale per raggiungere un obiettivo informativo.

14. Nel settore delle interfacce utente, tali elementi documentali possono trovarsi nella comunicazione di determinati accordi e, soprattutto, nell'ottenimento di elementi atti a dimostrare, ad esempio, l'espressione del consenso o la conferma di lettura.

2.2 Trasparenza

15. Il principio di trasparenza di cui all'articolo 5, paragrafo 1, lettera a), GDPR si sovrappone in larga misura all'ambito della responsabilizzazione generale. Sebbene i titolari del trattamento debbano proteggere determinate informazioni commerciali sensibili nei confronti di terzi, rendere la documentazione relativa al trattamento accessibile o registrabile potrebbe contribuire alla responsabilizzazione: ad esempio, per un testo che il titolare del trattamento deve mettere a disposizione conformemente al principio di trasparenza si può richiedere la conferma di lettura, che può servire anche a garantire nel contempo la trasparenza nei confronti degli interessati.

16. Tutti i principi in materia di protezione dei dati di cui all'articolo 5 GDPR sono specificati in dettaglio nel regolamento stesso. L'articolo 5, paragrafo 1, lettera a), GDPR stabilisce che i dati personali sono trattati in modo trasparente nei confronti dell'interessato. Le linee guida sulla trasparenza specificano gli elementi di trasparenza di cui all'articolo 12 GDPR, ossia la necessità di fornire le informazioni in "forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro"[18]. Le presenti linee guida forniscono inoltre orientamenti su come adempiere agli obblighi di informazione di cui agli articoli 13 e 14 GDPR per quanto riguarda i fornitori di social media.

17. Il testo relativo ai principi applicabili alla protezione dei dati di cui all'articolo 5, paragrafo 1, lettera a), GDPR e altre disposizioni normative specifiche all'interno del regolamento contengono maggiori dettagli relativi al principio di trasparenza, collegati a principi normativi specifici, ad esempio i requisiti speciali di trasparenza di cui all'articolo 7 GDPR riguardante l'ottenimento del consenso.

[18] Gruppo di lavoro articolo 29, linee guida sulla trasparenza ai sensi del regolamento 2016/679, approvate dall'EDPB https://www.rgpdmanager.it/wp-content/uploads/2020/01/wp260rev01_it.pdf.

2.3 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

18. L'articolo 25, paragrafo 1, GDPR specifica che i titolari del trattamento mettono in atto misure tecniche e organizzative adeguate volte ad attuare i principi di protezione dei dati, mentre l'articolo 25, paragrafo 2, GDPR chiarisce che tali misure sono attuate anche per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Nelle *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* sono elencati alcuni elementi chiave di cui i titolari del trattamento e i responsabili del trattamento devono tenere conto nell'adempiere agli obblighi in materia di protezione dei dati fin dalla progettazione per quanto riguarda una piattaforma di social media. Uno di questi è che, per quanto riguarda il principio della correttezza, le informazioni e le opzioni relative al trattamento dei dati devono essere fornite in modo obiettivo e neutrale, evitando formulazioni o meccanismi ingannevoli o manipolatori[19]. Le linee guida individuano, tra l'altro, elementi dei principi per la protezione dei dati per impostazione predefinita e per la protezione dei dati fin dalla progettazione che assumono ancor più rilevanza per quanto riguarda i modelli di progettazione ingannevoli[20]:

- autonomia – agli interessati dovrebbe essere garantito il massimo grado possibile di autonomia nel determinare l'utilizzo cui sono sottoposti i loro dati personali, nonché l'ambito di applicazione e le condizioni di tale utilizzo o trattamento;
- interazione – gli interessati devono essere in grado di comunicare ed esercitare i propri diritti in relazione ai dati personali trattati dal titolare;
- aspettativa – il trattamento dovrebbe corrispondere alle aspettative ragionevoli degli interessati;
- libertà di scelta – il titolare non dovrebbe "catturare" (*lock-in*) i propri utenti in modo scorretto. Qualora un servizio che prevede il trattamento di dati personali abbia natura proprietaria, gli utenti potrebbero essere “catturati” rispetto a tale servizio, il che può essere scorretto qualora pregiudichi la possibilità per gli interessati di esercitare il diritto alla portabilità dei dati ai sensi dell’articolo 20 GDPR;
- equilibrio dei rapporti di forza - tale equilibrio dovrebbe essere un obiettivo chiave della relazione tra titolare e interessato. Occorre evitare gli squilibri nei rapporti di forza e, qualora ciò non sia possibile, è necessario individuarli e tenerne conto al fine di adottare adeguate contromisure;
- assenza di prassi ingannevoli – le informazioni e le opzioni relative al trattamento dei dati devono essere fornite in modo obiettivo e neutrale, evitando formulazioni o meccanismi ingannevoli o manipolatori;
- veridicità – il titolare deve dichiarare le proprie modalità di trattamento dei dati personali e deve agire secondo quanto dichiarato in merito, senza fuorviare gli interessati.

[19] Cfr. le Linee guida 4/20219 sull'articolo 25 "Protezione dei dati fin dalla progettazione e per impostazione predefinita", pag. 19, punto 70.
[20] In sintesi; per l'elenco completo, cfr. *Linee guida sull'articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita*, punto 70.

19. Il rispetto dei requisiti relativi alla protezione dei dati per impostazione predefinita e alla protezione dei dati fin dalla progettazione è importante ai fini della valutazione dei modelli di progettazione ingannevoli, in quanto consentirebbe di evitarli fin dall'inizio. In effetti, un confronto tra un servizio e le interfacce associate e gli elementi riguardanti i principi della protezione dei dati per impostazione predefinita e per progettazione, come quelli di cui sopra, sarà utile per individuare gli aspetti del servizio che potrebbero costituire un modello di progettazione ingannevole prima del suo lancio. Ad esempio, se le informazioni sulla protezione dei dati sono fornite senza seguire il principio di "assenza di prassi ingannevoli", è probabile che si configuri un modello di progettazione ingannevole del tipo ***poca visibilità*** o ***stimolazione emotiva***, che saranno esaminati nel caso d'uso n. 1.

3 IL CICLO DI VITA DI UN ACCOUNT SUI SOCIAL MEDIA: METTERE IN PRATICA I PRINCIPI

20. Il GDPR si applica al trattamento automatizzato di dati personali nella sua interezza[21]. Nel caso del trattamento di dati personali nell'ambito della gestione delle piattaforme di social media, ciò comporta l'applicazione del GDPR e dei suoi principi all'intero ciclo di vita di un account utente.

3.1 Apertura di un account sui social media

Caso d'uso n. 1: registrazione di un account

a. Descrizione del contesto

21. Il primo passo che gli utenti devono compiere per avere accesso a una piattaforma di social media è l'iscrizione mediante la creazione di un account. Nell'ambito di questo processo di registrazione, gli utenti sono invitati a fornire i propri dati personali, quali nome e cognome, indirizzo e-mail o talvolta numero di telefono. Gli utenti devono essere informati del trattamento dei loro dati personali e di solito sono invitati a confermare di aver letto l'informativa sulla privacy e ad accettare le condizioni di utilizzo della piattaforma di social media. Tali informazioni devono essere fornite in un linguaggio semplice e chiaro, in modo che gli utenti siano in grado di comprenderle facilmente ed esprimere consapevolmente l'accettazione.

22. In questa fase iniziale del processo di iscrizione gli utenti dovrebbero comprendere ciò che stanno esattamente sottoscrivendo, nel senso che l'oggetto dell'accordo tra la piattaforma di social media e gli utenti dovrebbe essere descritto nel modo più chiaro e semplice possibile.

23. Pertanto i fornitori dei social media devono tenere conto della protezione dei dati fin dalla progettazione in modo efficace al fine di tutelare i diritti e le libertà degli interessati[22].

b. Disposizioni normative pertinenti

24. Nella progettazione delle proprie interfacce, i fornitori di social media devono assicurarsi di attuare correttamente i principi di cui all'articolo 5 GDPR. La trasparenza nei confronti degli interessati è sempre essenziale, ma lo è in modo particolare nella fase di creazione di un account su una piattaforma di social media. Rivestendo la posizione di titolare del trattamento o di responsabile del trattamento, le piattaforme di social media dovrebbero fornire agli utenti, al momento della loro iscrizione, le informazioni in modo efficace e conciso, nonché chiaramente distinte da altre informazioni non legate alla protezione dei dati[23]. Parte degli obblighi di trasparenza dei titolari del trattamento consiste nell'informare gli utenti in merito ai loro diritti, uno dei quali consiste nel revocare il proprio consenso in qualsiasi momento se il consenso è la base giuridica applicabile per il trattamento[24].

i. Consenso fornito nella fase del processo di iscrizione

25. Come stabilito dall'articolo 4, punto 11), e dall'articolo 7 GDPR, e chiarito al considerando 32, il consenso, quando viene scelto come base giuridica per il trattamento, deve essere

[21] Cfr. articolo 2, paragrafo 1, GDPR.
[22] Cfr. *Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita*.
[23] Cfr. linee guida sulla trasparenza, punto 8.
[24] Linee guida sulla trasparenza, punto 30 e pag. 39.

"*[una] manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*". Affinché il consenso possa essere considerato valido, devono essere soddisfatti tutti questi requisiti.

26. Per i fornitori di social media che chiedono il consenso degli utenti per diverse finalità di trattamento, le linee guida 5/2020 dell'EDPB sul consenso forniscono preziose indicazioni sull'ottenimento del consenso[25]. Le piattaforme di social media non devono eludere condizioni, quali la capacità degli interessati di prestare liberamente il proprio consenso, attraverso l'utilizzo di progettazioni grafiche o formule che impediscano agli interessati di esercitare tale volontà. A tale riguardo l'articolo 7, paragrafo 2, GDPR stabilisce che la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Gli utenti delle piattaforme di social media possono fornire il consenso per annunci pubblicitari o tipi speciali di analisi durante il processo di iscrizione e in una fase successiva attraverso le impostazioni relative alla protezione dei dati. In ogni caso, come sottolinea il considerando 32 GDPR, il consenso deve sempre essere espresso mediante un atto positivo inequivocabile, e pertanto non configura consenso l'inattività o la preselezione di caselle[26].

27. Come già evidenziato dalle linee guida dell'EDPB sul consenso, affinché il consenso sia "informato" agli utenti devono essere forniti alcuni elementi informativi minimi[27]. In caso contrario, il consenso acquisito durante il processo di iscrizione non può essere considerato valido ai sensi del GDPR, rendendo in tal modo illecito il trattamento.

28. Gli utenti sono invitati a prestare il proprio consenso per diversi tipi di finalità (ad esempio il trattamento di dati personali aggiuntivi). Il consenso non è specifico e quindi non è valido se gli utenti non ricevono in modo chiaro informazioni anche su ciò a cui stanno acconsentendo[28]. Come previsto dall'articolo 7, paragrafo 2, GDPR, il consenso dovrebbe essere richiesto in modo da essere chiaramente distinguibile dalle altre materie, a prescindere dal modo in cui le informazioni sono presentate all'interessato. In particolare, quando è richiesto per via elettronica, il consenso non deve essere incluso nelle condizioni generali di contratto/servizio[29]. Tenendo conto del fatto che un numero crescente di utenti accede alle piattaforme di social media utilizzando l'interfaccia dei propri smartphone per iscriversi alla piattaforma, i fornitori di social media devono prestare particolare attenzione al modo in cui è richiesto il consenso, per assicurarsi che tale consenso sia distinguibile. Gli utenti non devono trovarsi di fronte a una quantità di informazioni talmente elevata da indurli a evitarne la lettura. Per contro, nel caso in cui, per creare un account, gli utenti siano "tenuti" a confermare di aver letto l'intera politica in materia di privacy e ad accettare le condizioni generali di contratto/servizio del fornitore di social media, comprese tutte le operazioni di trattamento, si potrebbe configurare un consenso forzato alle condizioni particolari indicate in tale politica. Se il suo rifiuto comporta un diniego del servizio, il consenso non può essere considerato liberamente prestato, granulare e specifico, come previsto dal GDPR. Il consenso "accorpato" all'accettazione delle condizioni generali di contratto/servizio di un fornitore di social media non si può considerare "prestato

[25] EDPB, *Linee guida 5/2020 dell'EDPB sul consenso ai sensi del regolamento (UE) 2016/679,* versione 1.1, adottate il 4 maggio 2020 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_it.pdf.

[26] Cfr. Corte di giustizia dell'Unione europea, sentenza del 1º ottobre 2019, *Verbraucherzentrale Bundesverband e.V. contro Planet 49 GmbH*, causa C-673/17, ECLI:EU:C:2019:801, punti 62-63.

[27] Linee guida 5/2020 sul consenso, punto 64; cfr. anche il caso d'uso n. 3a della parte 3.3 delle presenti linee guida.

[28] Cfr. le Linee guida 5/2020 sul consenso, punto 68.

[29] Linee guida sulla trasparenza, punto 8.

liberamente"[30]. Ciò vale anche quando il titolare del trattamento "subordina" la fornitura di un contratto o servizio a una richiesta di consenso al trattamento di dati personali che non sono necessari per l'esecuzione del contratto o servizio.

29. Sebbene il consenso debba essere espresso mediante un'azione positiva da parte degli utenti, la mancanza di consenso dovrebbe essere considerata lo stato predefinito, fino a quando non sia stato prestato il consenso. L'espressione del rifiuto degli utenti non dovrebbe pertanto richiedere alcuna azione da parte loro o dovrebbe essere possibile attraverso un'azione che presenti lo stesso grado di semplicità di quella che consente di esprimere il proprio consenso[31].

ii. Revoca del consenso — articolo 7, paragrafo 3, GDPR

30. Conformemente all'articolo 7, paragrafo 3, prima frase, GDPR, gli utenti delle piattaforme di social media possono revocare il proprio consenso in qualsiasi momento. Prima di esprimere il proprio consenso, gli utenti devono inoltre essere informati di tale diritto, come previsto dall'articolo 7, paragrafo 3, terza frase, GDPR. In particolare, i titolari del trattamento devono dimostrare che gli utenti hanno la possibilità di rifiutare o revocare il consenso senza subire pregiudizio. Gli utenti delle piattaforme di social media che acconsentono al trattamento dei propri dati personali con un solo clic, ad esempio selezionando una casella, devono poter revocare il proprio consenso in modo altrettanto facile[32]. Tale aspetto conferma il fatto che il consenso dovrebbe essere una decisione reversibile, in modo che l'interessato mantenga un certo grado di controllo in relazione al rispettivo trattamento[33]. La facilità della revoca costituisce un prerequisito affinché un consenso sia considerato valido ai sensi dell'articolo 7, paragrafo 3, quarta frase, GDPR e dovrebbe essere possibile senza abbassare i livelli del servizio[34]. A titolo di esempio, il consenso non può essere considerato valido ai sensi del GDPR quando è espresso con un solo click di mouse, un solo scorrimento o premendo un tasto, mentre la revoca richiede più passaggi[35], è più difficile da portare a termine o richiede più tempo.

c. Modelli di progettazione ingannevoli

31. Il GDPR contiene molte disposizioni che attengono al processo di iscrizione. Esistono pertanto diversi modelli di progettazione ingannevoli che possono verificarsi se i fornitori di social media non attuano correttamente il regolamento.

i. Modelli basati sui contenuti

Overloading — Sollecitazione continua (lista di controllo 4.1.1 dell'allegato I)

32. Il modello di progettazione ingannevole della ***sollecitazione continua*** si ha quando, mediante ripetute richieste di fornire dati aggiuntivi o di prestare il consenso per una finalità di trattamento, gli utenti sono spinti a fornire più dati personali di quelli necessari per le finalità del trattamento o ad acconsentire a un altro uso dei propri dati. Tali ripetute sollecitazioni possono giungere attraverso uno

[30] Cfr.le Linee guida 8/2020 sul *targeting* degli utenti di social media, punto 57.
[31] Cfr. considerando 42, quinta frase, GDPR.
[32] Cfr. linee guida sulla trasparenza, punti 113 e segg.
[33] Linee guida 5/2020 sul consenso, punto 10.
[34] Linee guida 5/2020 sul consenso, punto 114.
[35]Cfr. le linee guida 5/2020 sul consenso, punto 114.

o più dispositivi. È probabile che, stanchi di dover respingere le richieste ogni volta che utilizzano la piattaforma, gli utenti finiscano per cedere.

Example 1:

Variante A: nella prima fase del processo di iscrizione l'utente deve scegliere tra due diverse opzioni per registrarsi. Può fornire un indirizzo e-mail oppure un numero di telefono. Se l'utente opta per l'indirizzo e-mail, il fornitore di social media cerca comunque di convincerlo a fornire il numero di telefono, dichiarando che sarà utilizzato per la sicurezza dell'account, senza fornire alternative in merito ai dati che l'utente potrebbe fornire o ha già fornito. In concreto, durante l'intero processo di iscrizione appaiono diverse finestre pop-up contenenti un campo per l'inserimento del numero di telefono, accompagnato dalla spiegazione "*Utilizzeremo il tuo numero [di telefono] per la sicurezza dell'account*". Sebbene possa chiudere tali finestre, l'utente è sovraccaricato e si arrende fornendo il suo numero di telefono.

Variante B: un altro fornitore di social media chiede ripetutamente all'utente di fornire il numero di telefono ogni volta che questi accede al proprio account nonostante l'utente si sia precedentemente rifiutato di fornirlo, indipendentemente dal fatto che ciò sia avvenuto durante il processo di iscrizione o in occasione dell'ultimo accesso.

33. L'esempio appena fornito illustra la situazione in cui agli utenti viene chiesto continuamente di fornire determinati dati personali, come il loro numero di telefono. Mentre nella variante A dell'esempio la ***sollecitazione continua*** è attuata più volte durante il processo di iscrizione, la variante B evidenzia che gli utenti possono trovarsi di fronte a questo modello di progettazione ingannevole anche quando sono già registrati. Per evitare questo modello è importante tenere particolarmente conto dei principi di minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), GDPR e, in casi come quello descritto nell'esempio 1, variante A, anche del principio di limitazione delle finalità di cui all'articolo 5, paragrafo 1, lettera b), GDPR. Pertanto, se dichiarano che utilizzeranno il numero di telefono "per la sicurezza dell'account", i fornitori di social media devono trattare il numero di telefono solo per tali finalità di sicurezza e non possono successivamente trattarlo in un modo che va oltre tali finalità iniziali.

34. Per rispettare il principio della minimizzazione dei dati, i fornitori di social media sono tenuti a non chiedere dati aggiuntivi, come il numero di telefono, quando i dati già forniti dagli utenti durante il processo di iscrizione sono sufficienti. Ad esempio, per garantire la sicurezza dell'account, è possibile rafforzare l'autenticazione senza il numero di telefono, tramite il semplice invio di un codice agli account di posta elettronica dell'utente o con diversi altri mezzi.

35. I fornitori di social network dovrebbero pertanto consentire agli utenti di riaccedere utilizzando mezzi per la sicurezza più semplici. Ad esempio il fornitore di social media può inviare agli utenti un numero di autenticazione attraverso un canale di comunicazione aggiuntivo, come un'applicazione di sicurezza precedentemente installata dagli utenti sul proprio telefono cellulare, ma senza chiedere il loro numero di cellulare. Anche l'autenticazione utente tramite indirizzi di posta elettronica è meno invasiva rispetto a quella tramite numero di telefono, in quanto gli utenti possono limitarsi a creare un nuovo indirizzo di posta elettronica specificamente per il processo di iscrizione e utilizzarlo principalmente in relazione al social network. Un numero di telefono non è invece intercambiabile con altrettanta facilità, essendo alquanto improbabile che gli utenti acquistino una nuova carta SIM o stipulino un nuovo contratto telefonico con il solo scopo di effettuare l'autenticazione.

36. Occorre tenere presente che, se lo scopo di tale richiesta è dimostrare che gli utenti sono legittimamente in possesso del dispositivo utilizzato per accedere al social network, tale obiettivo può

essere raggiunto con diversi mezzi e il numero di telefono è soltanto uno di essi. Pertanto l'indicazione di un numero di telefono può costituire solamente una delle opzioni facoltative a disposizione degli utenti. In definitiva, sono gli utenti a dover decidere se utilizzare tale mezzo come fattore di autenticazione. In particolare, i numeri di telefono degli utenti non sono necessari per una verifica una tantum, in quanto l'indirizzo e-mail costituisce il normale punto di contatto con gli utenti durante il processo di registrazione.

37. La pratica illustrata nella variante A dell'esempio 1 può indurre l'utente in errore e portarlo a fornire inconsapevolmente l'informazione in questione, ritenendola necessaria per attivare o proteggere l'account. In realtà all'utente non è mai stata offerta alcuna alternativa (ad esempio l'uso dell'e-mail a fini di attivazione dell'account e di sicurezza). Nella variante B dell'esempio 1 l'utente non è informato in merito a una finalità del trattamento. Tuttavia questa variante costituisce comunque un modello di progettazione ingannevole di ***sollecitazione continua***, in quanto il fornitore di social media non tiene conto del fatto che in precedenza l'utente si è rifiutato di fornire il numero di telefono e continua a chiederglielo. Se l'utente ha l'impressione di poter evitare tale ripetuta richiesta soltanto inserendo i propri dati, è probabile che finisca per cedere.

38. Nell'esempio seguente gli utenti sono ripetutamente invitati a consentire alla piattaforma di social media di accedere ai loro contatti.

> **Example 2:** Una piattaforma di social media utilizza un'icona con il simbolo "informazioni" o con un punto interrogativo per sollecitare gli utenti a compiere l'azione "facoltativa" in quel momento richiesta. Tuttavia, anziché limitarsi a fornire informazioni agli utenti che si aspettano aiuto da questi pulsanti, la piattaforma sollecita gli utenti stessi ad accettare di importare i contatti dal proprio account di posta elettronica mostrando ripetutamente una finestra pop-up con la scritta "*Avanti!*".

39. Soprattutto nella fase del processo di iscrizione, la ***sollecitazione continua*** può indurre gli utenti ad accettare la richiesta della piattaforma pur di portare finalmente a termine l'iscrizione. L'effetto di questo modello di progettazione ingannevole si amplifica se combinato con un linguaggio motivazionale che aggiunge un senso di urgenza, come nell'esempio precedente.

40. Gli effetti condizionanti del linguaggio o delle immagini saranno trattati più avanti, in sede di esame del modello di progettazione ingannevole della ***stimolazione emotiva***[36].

Obstructing — Azione ingannevole (lista di controllo 4.4.3 dell'allegato I)

41. Un altro esempio di situazione in cui i fornitori di social media chiedono immotivatamente i numeri di telefono degli utenti riguarda l'uso dell'applicazione di una piattaforma.

> **Example 3:** Quando si iscrivono a una piattaforma di social media tramite un browser per desktop, gli utenti sono invitati a utilizzare anche l'applicazione mobile della piattaforma. Durante quello che sembra un altro passaggio del processo di iscrizione, gli utenti sono invitati a scoprire l'app. Quando cliccano sull'icona aspettandosi di essere rinviati a un app store, viene loro invece chiesto di fornire il numero per ricevere un messaggio di testo con il link all'applicazione.

[36] Cfr. i punti 43 e seguenti nel caso d'uso 1, nonché la panoramica degli esempi nella lista di controllo di cui all'allegato.

42. Spiegare agli utenti che devono fornire il numero di telefono per ricevere un link tramite cui scaricare l'applicazione costituisce un'***azione ingannevole*** per una serie di motivi: in primo luogo, gli utenti hanno a disposizione diversi modi per utilizzare un'applicazione, ad esempio scansionando un codice QR, utilizzando un link o scaricando l'applicazione dall'app store. In secondo luogo, queste soluzioni dimostrano che il fornitore della piattaforma di social media non ha alcun motivo inderogabile per richiedere il numero di telefono degli utenti. Una volta completato il processo di iscrizione, gli utenti devono potersi connettere utilizzando i propri dati di login (solitamente l'indirizzo e-mail e la password) da qualsiasi dispositivo, a prescindere che utilizzino un browser per desktop, un browser per dispositivi mobili o un'applicazione. Ciò è tanto più vero se si considera che, invece che su uno smartphone, gli utenti potrebbero desiderare di installare l'applicazione sul proprio tablet, un dispositivo non collegato a un numero di telefono.

Stirring — Stimolazione emotiva (lista di controllo 4.3.1 dell'allegato I)

43. Con il modello di progettazione ingannevole della ***stimolazione emotiva***, i testi o gli elementi visivi (ad esempio stile, colori, immagini o altro) sono utilizzati in modo da trasmettere le informazioni agli utenti in una prospettiva molto positiva che li fa sentire bene, al sicuro o ricompensati, o molto negativa, che infonde ansia, li fa sentire colpevoli o puniti. Il modo in cui le informazioni sono presentate agli utenti influenza il loro stato emotivo e potrebbe indurli ad agire contro i propri interessi in materia di protezione dei dati. L'impatto di tali pratiche può essere ancora più efficace se basato sui dati raccolti dalla piattaforma. Influenzare le scelte degli individui fornendo loro informazioni distorte può generalmente essere considerata una pratica scorretta contraria al principio di correttezza del trattamento di cui all'articolo 5, paragrafo 1, lettera a), GDPR. È una pratica che può interessare l'intero percorso dell'utente all'interno di una piattaforma di social media. Tuttavia, nella fase del processo di iscrizione, l'effetto condizionante può essere particolarmente forte, considerando il sovraccarico di informazioni che gli utenti potrebbero dover gestire in aggiunta ai passaggi necessari per completare la registrazione.

44. Alla luce di quanto precede, la ***stimolazione emotiva*** nella fase della registrazione presso una piattaforma di social media può avere un impatto ancora maggiore sui minori, sugli anziani e su altri gruppi (ossia portarli a fornire un maggior numero di dati personali a causa della mancanza di comprensione delle attività di trattamento), data la loro natura di interessati vulnerabili[37]. Quando i servizi di una piattaforma di social media sono rivolti ai minori o ad altri interessati vulnerabili, dovrebbe essere garantito l'utilizzo di un linguaggio adeguato, anche nel tono e nello stile, in modo che gli utenti vulnerabili, in quanto destinatari del messaggio, comprendano facilmente le informazioni fornite[38]. In ragione della loro vulnerabilità, i minori, gli anziani e altri interessati possono essere indotti dai modelli di progettazione ingannevoli a condividere maggiori informazioni, in quanto espressioni "perentorie" possono portarli a sentirsi obbligati a farlo, ad esempio per apparire popolari tra i propri pari o perché ritengono che la fornitura dei dati sia obbligatoria.

45. Quando sono spinti ad affrettarsi a fornire i propri dati, gli utenti delle piattaforme di social media non hanno il tempo di "elaborare" e quindi di comprendere realmente le informazioni ricevute per poter prendere una decisione consapevole. Il linguaggio motivazionale utilizzato dalle piattaforme di social media potrebbe indurre gli utenti a fornire di conseguenza più dati di quelli necessari, se pensano che

[37] Cfr. anche il punto 7.

[38] Cfr. linee guida sulla trasparenza, punto 18.

quanto proposto dalla piattaforma di social media sia ciò che farà la maggior parte degli utenti e quindi il "modo corretto" di procedere.

> **Example 4:** Utilizzando il messaggio seguente, la piattaforma di social media chiede agli utenti di condividere la loro geolocalizzazione: "Ehi, sei un lupo solitario, vero? Ma la condivisione e la connessione con gli altri contribuiscono a rendere il mondo un luogo migliore! Condividi la tua geolocalizzazione! Lasciati ispirare dai luoghi e dalle persone che ti circondano!"

46. Durante il processo di iscrizione, l'obiettivo degli utenti è completare la registrazione per poter utilizzare la piattaforma di social media. In questo contesto gli effetti di modelli di progettazione ingannevoli come la ***stimolazione emotiva*** si amplificano. La loro potenza può essere ancora maggiore a metà o verso la fine del processo di iscrizione rispetto all'inizio dello stesso, in quanto gli utenti completeranno nella maggior parte dei casi tutti i passaggi necessari "in fretta" o saranno più esposti a un senso di urgenza. In tale contesto gli utenti sono più propensi ad accettare di inserire tutti i dati che vengono loro richiesti, senza prendersi il tempo necessario per chiedersi se debbano farlo. In tal senso, il linguaggio motivazionale utilizzato dal fornitore di social media può indurre gli utenti a decidere seduta stante. Lo stesso dicasi per la combinazione del linguaggio motivazionale con altre forme enfatiche, quali i punti esclamativi, come illustrato nell'esempio che segue.

> **Example 5:** Il fornitore di social media invita gli utenti a condividere più dati personali di quelli effettivamente necessari, sollecitandoli a fornire un'autodescrizione: "*Raccontaci di te! Forza, non vediamo l'ora di conoscerti!*

47. Grazie a questa prassi, le piattaforme di social media ricevono un profilo più dettagliato dei loro utenti. Tuttavia, a seconda dei casi, la fornitura di un maggior numero di dati personali, riguardanti ad esempio la personalità degli utenti, potrebbe non essere necessaria per la fruizione del servizio in sé e pertanto violerebbe il principio di minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), GDPR. Come illustrato nell'esempio 5, tali tecniche non contribuiscono alla libera volontà degli utenti di fornire i propri dati, in quanto il linguaggio prescrittivo utilizzato può far sì che gli utenti si sentano obbligati a fornire un'autodescrizione, poiché hanno già dedicato tempo alla registrazione e desiderano completarla. Durante il processo di registrazione su un account, è meno probabile che gli utenti si fermino per riflettere sulla descrizione che forniscono o per pensare se desiderano darne una, tanto più se il linguaggio utilizzato trasmette un senso di urgenza o di indispensabilità. Se gli utenti percepiscono la fornitura dei dati come obbligatoria, anche quando in realtà non lo è, ciò influisce sulla loro "libera volontà". Significa inoltre che le informazioni fornite dalla piattaforma dei social media non erano chiare.

> **Example 6:** La parte del processo di iscrizione in cui gli utenti sono invitati a caricare la loro immagine contiene un pulsante "?". Cliccando su di esso appare il seguente messaggio: "*Non è necessario andare prima a farsi belli. Basta scegliere una foto che dice "eccomi"."*

48. Anche se le frasi dell'esempio 6 mirano a motivare gli utenti e in apparenza a semplificare il processo a loro vantaggio (ossia, non serve una foto ufficiale per la registrazione), tali pratiche possono incidere sulla decisione finale presa dagli utenti che avevano inizialmente deciso di non condividere una foto per il loro account. I punti interrogativi sono utilizzati per le domande e, cliccando su un'icona con un punto interrogativo, gli utenti possono aspettarsi di trovare informazioni utili. Quando tale aspettativa non è soddisfatta e gli utenti sono invece spinti per l'ennesima volta a compiere azioni rispetto alle quali sono titubanti, il consenso raccolto senza informare gli utenti in merito al trattamento della loro immagine non sarebbe valido, in quanto non soddisfa i requisiti del consenso "informato" e

"liberamente prestato" ai sensi dell'articolo 7 GDPR, in combinato disposto con l'articolo 4, punto 11), GDPR. Il fattore emotivo incide quindi fortemente sulla legittimità del consenso.

Obstructing — Allungare più del necessario (lista di controllo 4.4.2 dell'allegato I)

49. Quando gli utenti cercano di attivare un controllo relativo alla protezione dei dati, ma il percorso è impostato in modo da richiedere il completamento di un numero di passaggi superiore rispetto a quello necessario per l'attivazione di scelte invasive riguardo ai dati, si configura il modello di progettazione ingannevole dell'***allungare più del necessario***. È probabile che questo modello scoraggi gli utenti dall'attivare i controlli di protezione dei dati. Nel processo di iscrizione, ciò può tradursi nella visualizzazione di una finestra pop-in o pop-up che chiede agli utenti di confermare la propria decisione quando scelgono un'opzione restrittiva (ad esempio se scelgono di rendere privati i propri profili). L'esempio che segue illustra un altro caso in cui un processo di iscrizione è ***allungato più del necessario***.

> **Example 7:** Durante il processo di iscrizione, agli utenti che cliccano sui pulsanti "salta" per evitare di inserire un certo tipo di dati appare una finestra pop-up che chiede "*Sei sicuro*?". Mettendo in discussione la loro decisione e quindi sollevando dubbi in merito, il fornitore di social media spinge gli utenti a ritornare sulla propria scelta e divulgare questo tipo di dati, come il genere di appartenenza, il proprio elenco dei contatti o la propria immagine. Agli utenti che scelgono di inserire direttamente i dati non appare invece alcun messaggio che chieda di riconsiderare la propria scelta.

In questo caso, chiedere agli utenti di confermare di non voler compilare un campo di dati può indurli a tornare sulla decisione iniziale e a inserire i dati richiesti. Ciò vale in particolare per gli utenti che non hanno familiarità con le funzioni della piattaforma di social media. Il modello di progettazione ingannevole dell'***allungare più del necessario*** tenta di influenzare le decisioni degli utenti rallentandoli e mettendo in discussione la loro scelta iniziale, oltre a prolungare immotivatamente il processo di iscrizione, il che costituisce una violazione del principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR. L'esempio mostra che il modello di progettazione ingannevole può indurre gli utenti a divulgare una quantità di dati personali anche maggiore di quella scelta inizialmente. Descrive uno squilibrio fra il trattamento degli utenti che divulgano i dati personali immediatamente e quello degli utenti che non lo fanno: soltanto coloro che si rifiutano di divulgare i dati sono invitati a confermare la propria scelta, mentre gli utenti che li divulgano non sono invitati a confermarla. Ciò costituisce una violazione del principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR rispetto agli utenti che non desiderano divulgare questo tipo di dati personali.

ii. Modelli basati sull'interfaccia

Stirring — Poca visibilità (lista di controllo 4.3.2 dell'allegato I)

50. In virtù del principio di trasparenza, agli interessati devono essere fornite informazioni chiare che consentano loro di comprendere come i loro dati personali sono trattati e come possono controllarli. Inoltre tali informazioni devono essere facilmente individuabili dagli interessati. Tuttavia le informazioni relative alla protezione dei dati, in particolare i link, sono spesso visualizzate in modo tale da passare facilmente inosservate. Tali pratiche di ***poca visibilità*** utilizzano uno stile di visualizzazione

dei controlli delle informazioni o della protezione dei dati che porta l'utente a sorvolare sulle opzioni che favoriscono la protezione dei dati a vantaggio di opzioni meno restrittive e quindi più invasive.

51. L'utilizzo di caratteri di piccole dimensioni o di un colore che non contrasta abbastanza da offrire una leggibilità adeguata (ad esempio un testo grigio chiaro su sfondo bianco) può avere un impatto negativo sugli utenti, in quanto il testo sarà meno visibile e gli utenti lo trascureranno o avranno difficoltà a leggerlo. Ciò vale in particolare quando uno o più elementi che attirano l'attenzione sono collocati accanto alle informazioni obbligatorie relative alla protezione dei dati. Queste tecniche di interfaccia inducono gli utenti in errore e rendono più impegnativo e dispendioso in termini di tempo individuare le informazioni relative alla protezione dei loro dati, in quanto per individuare le informazioni pertinenti occorrono più tempo e meticolosità.

> **Example 8:** Subito dopo aver completato la registrazione, gli utenti possono accedere alle informazioni sulla protezione dei dati solo aprendo il menu principale della piattaforma di social media e consultando la sezione del sottomenu che contiene un link alle "*impostazioni relative alla privacy e ai dati*". Una volta entrati nella pagina, il link alla politica sulla privacy non è visibile a prima vista. Gli utenti devono scorgere, in un angolo della pagina, una minuscola icona che indica la politica sulla privacy, pertanto difficilmente potranno individuare dove si trovano le informazioni relative alle politiche in materia di protezione dei dati.

52. È importante osservare che, anche quando i fornitori di social media rendono disponibili tutte le informazioni che devono essere fornite agli interessati a norma degli articoli 13 e 14 GDPR, le modalità di presentazione di tali informazioni possono comunque violare i requisiti generali di trasparenza di cui all'articolo 12, paragrafo 1, GDPR. Quando sono ***poco visibili*** e quindi possono sfuggire, le informazioni generano confusione o disorientamento e quindi non possono essere considerate comprensibili e facilmente accessibili, per cui sono incompatibili con l'articolo 12, paragrafo 1, GDPR.

53. Sebbene il precedente esempio mostri il modello di progettazione ingannevole dopo il completamento del processo di iscrizione, tale modello si riscontra già durante il processo di iscrizione, come sarà illustrato nell'esempio seguente che combina il modello della ***poca visibilità*** con quello della ***comodità ingannevole***.

Skipping — Comodità ingannevole (lista di controllo 4.2.1 dell'allegato I)

54. I fornitori di social media devono anche tenere presente il principio della protezione dei dati per impostazione predefinita. Quando le impostazioni dei dati sono preselezionate, gli utenti sono soggetti a uno specifico livello di protezione dei dati, determinato per impostazione predefinita dal fornitore piuttosto che dagli utenti stessi. Inoltre agli utenti non è sempre offerta immediatamente la possibilità di modificare le impostazioni scegliendo impostazioni più restrittive e conformi alla protezione dei dati. Il rispetto del GDPR a tale riguardo non implica che tutte le opzioni debbano apparire esattamente uguali. Tuttavia, se i fornitori di social media mettono in evidenza una delle opzioni e quindi attirano su di essa l'attenzione degli utenti, deve trattarsi di quella più restrittiva per quanto riguarda i dati personali, al fine di rispettare, tra l'altro, il principio della minimizzazione dei dati di cui all'articolo 5, paragrafo 1, lettera c), GDPR.

55. Quando le funzioni e le opzioni più invasive riguardanti i dati sono attivate per impostazione predefinita, si configura il modello della ***comodità ingannevole***. A causa dell'effetto dell'impostazione predefinita che spinge i singoli a mantenere un'opzione preselezionata, è improbabile che, benché ne

abbiano la possibilità, gli utenti modifichino tali opzioni. Si tratta di una pratica che si incontra comunemente nei processi di iscrizione, come illustrato nell'esempio 9, in quanto rappresenta un modo efficace per attivare opzioni invasive riguardo ai dati che altrimenti probabilmente gli utenti rifiuterebbero. Tali modelli di progettazione ingannevoli violano il principio della protezione dei dati per impostazione predefinita di cui all'articolo 25, paragrafo 2, GDPR, in particolare quando incidono sulla raccolta di dati personali, sulla portata del trattamento, sul periodo di conservazione e sull'accessibilità dei dati[39].

Example 9: In questo esempio, quando inserisce la data di nascita l'utente è invitato a scegliere con chi condividere tali informazioni. Benché siano disponibili opzioni meno invasive, l'opzione *"share it with everyone" (condividi con tutti)* è selezionata per impostazione predefinita, il che significa che tutti, ossia gli utenti registrati e tutti gli utenti di internet, potranno vedere la data di nascita dell'utente.

[39] Cfr. anche il punto 446 della decisione finale dell'autorità irlandese per la protezione dei dati relativa a Instagram (Meta Platforms Ireland Limited) a seguito della decisione vincolante di risoluzione delle controversie dell'EDPB del 28 luglio 2022, https://edpb.europa.eu/news/news/2022/record-fine-instagram-following-edpb-intervention_it.

56. L'esempio 9 mostra un modello di ***comodità ingannevole***, in quanto a essere selezionata, e quindi attivata, per impostazione predefinita non è l'opzione che offre il massimo livello di protezione dei dati. Inoltre l'effetto dell'impostazione predefinita di questo modello spinge gli utilizzatori a mantenere la preselezione, ossia a non prendersi tempo per esaminare le altre opzioni in questa fase né per tornare a modificare l'impostazione in una fase successiva. In questa interfaccia è utilizzato anche il modello della ***poca visibilità***. Infatti inserire la data di nascita non è obbligatorio, in quanto l'utente può saltare questo passaggio dell'iscrizione cliccando sul link "*Skip this step and sign up" (salta questo passaggio e registrati)*, disponibile sotto il pulsante "*Join the network!" (entra a far parte della rete!)*. Il fatto che il campo relativo alla data di nascita e il pulsante di conferma siano così visibili è tale da indurre l'utente a inserire la data di nascita e a inviarla al social network, in quanto non nota la possibilità di non condividere tali informazioni. Questo effetto sarebbe ancora più accentuato se si utilizzassero cerchi animati accanto al campo e al pulsante, che attirino molto l'attenzione degli utenti.

57. Il rispetto del principio della protezione dei dati fin dalla progettazione e per impostazione predefinita non implica che tutte le opzioni offerte debbano apparire esattamente uguali. Tuttavia, se i titolari del trattamento decidono di mettere in risalto un'opzione più delle altre, quella evidenziata deve essere la più restrittiva per quanto riguarda il trattamento dei dati.

58. Oltre a indurre gli utenti a mantenere un'opzione che non corrisponde necessariamente alle loro preferenze, i fornitori di social media potrebbero non invitare gli utenti a verificare o modificare le proprie impostazioni di protezione dei dati in base alle proprie preferenze dopo il completamento del processo di iscrizione. Inoltre la modifica di tali impostazioni predefinite potrebbe richiedere diversi passaggi. Quando gli utenti non sono in alcun modo invitati a verificare o modificare le proprie impostazioni di protezione dei dati o non sono indirizzati in modo chiaro alle relative informazioni, il livello di protezione dei loro dati dipenderà dalla loro iniziativa. Per facilitare il controllo dei propri dati da parte degli utenti, è possibile utilizzare i cosiddetti pannelli di controllo della privacy concepiti per centralizzare e facilitare tale operazione.

59. È importante tenere presente che la mancanza di protezione dei dati fin dalla progettazione e per impostazione predefinita, in combinazione con l'effetto dell'impostazione predefinita sopra illustrato, può avere conseguenze dannose per gli interessati, anche per quanto riguarda la loro sicurezza informatica. La visualizzazione pubblica di dati personali, come la data di nascita, utilizzati per i processi di verifica da parte di altri servizi online potrebbe facilitare l'accesso di criminali agli acquisti, alle banche e ad altri conti degli utenti. Un'altra conseguenza dannosa riguarda le possibilità di contatto sulla piattaforma dei social media: se l'opzione predefinita per l'invio di richieste di contatto o messaggi agli utenti è impostata su "tutti", il rischio di adescamento informatico e frodi è maggiore, in particolare per i gruppi vulnerabili.

60. Infine, se la ***comodità ingannevole*** è applicata all'ottenimento del consenso, il che equivarrebbe a ritenere che gli utenti acconsentano per impostazione predefinita, ad esempio utilizzando una casella preselezionata o considerando l'inerzia come approvazione, le condizioni per il consenso di cui all'articolo 4, punto 11), GDPR non sono soddisfatte e il trattamento sarebbe considerato illecito ai sensi dell'articolo 5, paragrafo 1, lettera a), e dell'articolo 6, paragrafo 1, lettera a), GDPR.

Obstructing — Punto morto (lista di controllo 4.4.1 dell'allegato I)

61. È importante sottolineare che la fase del processo di iscrizione è un momento determinante per informare gli utenti. Se sono alla ricerca di informazioni e non riescono a trovarle in quanto non è

disponibile o non funziona alcun link di reindirizzamento, si configura un modello di ***punto morto*** perché gli utenti non sono messi in condizione di raggiungere tale obiettivo.

> **Example 10:** Una volta avviato il processo di iscrizione, agli utenti non è fornito alcun link alle informazioni sulla protezione dei dati. Non riescono a trovarlo, in quanto non è fornito in nessun punto dell'interfaccia di registrazione, nemmeno in calce.

62. In pratica, nella situazione dell'esempio gli utenti avranno soltanto la possibilità di interrompere la registrazione e tornare alla pagina iniziale, se questa contiene un link all'informativa sulla privacy, oppure completare la registrazione, accedere alla piattaforma dei social media e solo successivamente avere accesso alle informazioni relative alla protezione dei dati. Ciò viola il principio di trasparenza e di facile accesso alle informazioni che devono essere fornite agli interessati, previsto dall'articolo 12, paragrafo 1, GDPR. Non sono soddisfatti inoltre i requisiti di cui all'articolo 13, paragrafi 1, e 2, GDPR, in quanto nel momento in cui i dati personali sono ottenuti non è fornita o resa accessibile alcuna informazione.

63. Un'altra modalità con cui può verificarsi il modello del ***punto morto*** si ha quando durante il processo di iscrizione gli utenti hanno a disposizione un'azione o un'opzione relativa alla protezione dei dati che successivamente, durante l'utilizzo del servizio, non riescono più a trovare.

> **Example 11:** Durante il processo di iscrizione gli utenti possono acconsentire al trattamento dei propri dati personali a fini pubblicitari e sono informati della possibilità di modificare la propria scelta in qualunque momento dopo la registrazione accedendo alla sezione della politica sulla privacy. Tuttavia, una volta completato il processo di registrazione e aperta la sezione della politica sulla privacy, gli utenti non trovano strumenti o indicazioni utili per revocare il consenso a tale trattamento.

64. In questo esempio specifico, gli utenti non hanno la possibilità di revocare il proprio consenso una volta registrati. In questo caso il modello di progettazione ingannevole del ***punto morto*** viola il diritto degli interessati di revocare il consenso in qualsiasi momento e con la stessa facilità con cui è accordato, ai sensi dell'articolo 7, paragrafo 3, prima e quarta frase, GDPR.

65. Infine anche indicare agli utenti un link che dovrebbe condurli a pagine relative alla protezione dei dati, come le impostazioni o le informazioni sulla protezione dei dati, costituisce un esempio di modello di ***punto morto*** se il link non funziona e non sono forniti link alternativi che aiutino gli utenti a trovare ciò che cercano. In questo modo gli utenti non possono cercare le informazioni pertinenti, né viene loro fornita alcuna spiegazione, come il motivo per cui ciò avviene (ad esempio problemi tecnici). In tal caso si delineano gli stessi problemi relativi alla trasparenza e alla facilità di accesso alle informazioni descritti al punto 58.

d. Migliori prassi

Per progettare interfacce utente che facilitino l'efficace attuazione del GDPR, l'EDPB raccomanda di attuare, per il processo di iscrizione, le migliori prassi indicate di seguito.

Scorciatoie: i link a informazioni, azioni o impostazioni che possono essere di aiuto pratico agli utenti nella gestione dei loro dati e delle loro impostazioni di protezione dei dati dovrebbero essere disponibili ogni qualvolta gli utenti si trovino di fronte a informazioni o esperienze correlate a tali aspetti (*ad esempio link che reindirizzano alle parti pertinenti della politica sulla privacy*).

Informazioni di contatto: l'indirizzo di contatto della società a cui inviare le richieste di protezione dei dati dovrebbe essere chiaramente indicato nella politica sulla privacy. Dovrebbe essere presente in

una sezione in cui gli utenti possono aspettarsi di trovarlo, ad esempio una sezione sull'identità del responsabile del trattamento dei dati, una sezione relativa ai diritti o una dedicata ai contatti.

Indicazioni per contattare l'autorità di controllo: indicare l'identità specifica dell'autorità di controllo e includere un link al suo sito web o alla pagina web specifica relativa alla presentazione di un reclamo. Tali informazioni dovrebbero essere presenti in una sezione in cui gli utenti possono aspettarsi di trovarle, ad esempio una sezione relativa ai diritti.

Panoramica della politica sulla privacy: all'inizio/nella parte superiore della pagina della politica sulla privacy, includere un indice (a tendina) con voci e sottovoci che mostri le diverse sezioni contenute nell'informativa sulla privacy. I nomi delle singole sezioni indicano chiaramente agli utenti l'esatto contenuto delle stesse, consentendo loro di individuare rapidamente la sezione desiderata e di accedervi.

Individuazione e confronto delle modifiche: quando sono apportate modifiche all'informativa sulla privacy, rendere accessibili le versioni precedenti con la relativa data di pubblicazione ed evidenziare le modifiche.

Formulazioni coerenti: in tutto il sito web sono utilizzate le stesse parole e la stessa definizione per un determinato aspetto della protezione dei dati. Le espressioni utilizzate nella politica sulla privacy dovrebbero corrispondere a quelle utilizzate sul resto della piattaforma.

Fornitura di definizioni: quando si utilizzano parole o un gergo non familiari o tecnici, fornire una definizione in un linguaggio semplice aiuterà gli utenti a comprendere le informazioni loro comunicate. La definizione può essere riportata direttamente nel testo, comparendo quando l'utente passa il cursore sulla parola, come pure essere resa disponibile in un glossario.

Messa in evidenza degli elementi relativi alla protezione dei dati: rendere visivamente evidenti elementi o azioni collegati alla protezione dei dati in un'interfaccia non direttamente dedicata a tale aspetto. Ad esempio, quando si pubblica un messaggio pubblico sulla piattaforma, i controlli sull'associazione della geolocalizzazione dovrebbero essere direttamente disponibili e chiaramente visibili.

Protezione dei dati nella fase di *onboarding*: il fornitore di social media può includere nell'esperienza di *onboarding* immediatamente successiva alla creazione di un account una serie di momenti relativi alla protezione dei dati per consentire agli utenti di scoprire e impostare agevolmente le proprie preferenze. Può ad esempio invitarli a impostare le preferenze riguardo alla protezione dei dati dopo l'aggiunta del primo amico o la condivisione del primo post.

Uso di esempi: oltre alle informazioni obbligatorie che indicano in modo chiaro e preciso la finalità del trattamento, per illustrare un trattamento specifico dei dati e renderlo più concreto per gli utenti si possono utilizzare esempi.

Informazioni contestuali: oltre a un'esaustiva politica sulla privacy, fornire brevi informazioni nel momento più opportuno affinché l'utente resti costantemente e precisamente informato sulle modalità di trattamento dei propri dati.

3.2 Stare in modo informato sui social media

Caso d'uso n. 2a: informativa sulla privacy a più livelli

a. **Descrizione del contesto**

66. Come già sottolineato nelle linee guida sulla trasparenza, il principio di trasparenza è strettamente legato al principio della correttezza del trattamento dei dati personali[40]. Tuttavia le informazioni relative al trattamento dei dati personali fanno anche sì che i responsabili del trattamento riflettano sulle proprie azioni, rendono il trattamento dei dati più comprensibile per gli interessati e, in ultima analisi, conferiscono a questi ultimi il potere di esercitare il controllo sui propri dati, in particolare mediante l'esercizio dei propri diritti. La conseguente perequazione delle capacità dei soggetti coinvolti conduce a un sistema corretto di trattamento dei dati personali. Tuttavia un maggior numero di informazioni non implica necessariamente una migliore informazione. Troppe informazioni irrilevanti o fuorvianti possono nascondere punti importanti del contenuto o ridurre la probabilità di trovarli. Pertanto, sotto questo profilo, il giusto equilibrio tra contenuto e presentazione comprensibile è fondamentale. Se tale equilibrio non è raggiunto, possono verificarsi modelli di progettazione ingannevoli.

b. **Disposizioni normative pertinenti**

67. I rapporti appena illustrati appaiono evidenti alla luce dell'articolo 5 GDPR. La trasparenza e la correttezza sono già sistematicamente menzionate l'una accanto all'altra nell'articolo 5, paragrafo 1, lettera a), GDPR, in quanto l'una determina l'altra. Il fatto che debba esistere non solo una trasparenza esterna ma anche interna è altresì chiarito dal requisito di responsabilizzazione di cui all'articolo 5, paragrafo 2, GDPR. La parte più importante della trasparenza interna è l'obbligo di tenere un registro delle attività di trattamento a norma dell'articolo 30 GDPR. Ai fini della trasparenza esterna, i fornitori di social media possono fornire agli utenti, tra l'altro, un'informativa sulla privacy a più livelli[41]. Tale necessità di comprensibilità e di correttezza del trattamento si traduce anche nei requisiti di cui all'articolo 12, paragrafo 1, GDPR, secondo cui le informazioni di cui agli articoli 13 e 14 GDPR sono fornite in forma concisa, trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Di conseguenza il contenuto delle informazioni deve essere reso disponibile senza ostacoli. Se i requisiti di cui all'articolo 12 GDPR non sono soddisfatti, le informazioni non sono valide ai sensi degli articoli 13 e 14 del GDPR. Pertanto, ai fini di un controllo efficace, i titolari del trattamento e i responsabili del trattamento possono essere chiamati a rispondere delle proprie azioni, in pratica dando così efficacia agli obblighi previsti dal GDPR.

c. Modelli di progettazione ingannevoli

i. Modelli basati sui contenuti

68. Per quanto riguarda il presente caso d'uso, i limiti dei modelli basati sul contenuto sono delineati nell'articolo 12, paragrafo 1, GDPR, che richiede una forma precisa e intelligibile nonché un linguaggio chiaro e semplice per quanto riguarda le informazioni fornite.

Left in the dark — Informazioni contrastanti (lista di controllo 4.6.2 dell'allegato I)

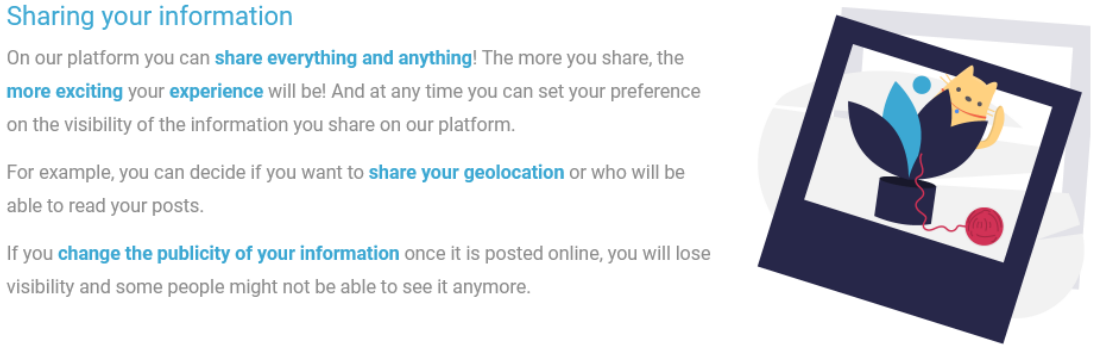
69. Uno dei casi più evidenti in cui questo modello può verificarsi si ha quando sono date ***informazioni contrastanti*** che lasciano l'utente nell'incertezza sul da farsi e sulle conseguenze delle proprie azioni, portandolo quindi a non compiere alcuna azione o a mantenere le impostazioni predefinite.

70. Le violazioni che tale situazione comporta, come la violazione dell'articolo 12, paragrafo 1, GDPR, possono essere anche amplificate, ad esempio, dall'effetto della ***stimolazione emotiva***. In linea di principio, testi, immagini e colori motivazionali sono consentiti, così come lo sono le pubblicità

[40] Linee guida sulla trasparenza, pagg. 4-5.

[41] Cfr. il caso d'uso n. 2.a nella sezione 3.2.

accattivanti. Essi potrebbero tuttavia amplificare l'effetto dei modelli di progettazione ingannevoli anche sotto il profilo del trattamento non corretto ai sensi dell'articolo 5, paragrafo 1, lettera a), GDPR.



Example 12: Nell'esempio fornito, le informazioni relative alla condivisione dei dati danno una visione estremamente positiva del trattamento, evidenziando i vantaggi della condivisione del maggior numero possibile di dati. Associato alla fotografia di un dolce animaletto che gioca con una pallina, questo tipo di ***stimolazione emotiva*** può dare agli utenti l'illusione di sicurezza e tranquillità per quanto riguarda i potenziali rischi derivanti dalla condivisione di qualche genere di informazioni sulla piattaforma. D'altro canto, le informazioni fornite su come controllare la pubblicità dei propri dati non sono chiare. All'inizio si afferma che gli utenti possono impostare la propria preferenza riguardo alla condivisione quando lo desiderano. Nell'ultima frase si dice però che non è possibile modificare la preferenza su un contenuto già pubblicato sulla piattaforma. Queste ***informazioni contrastanti*** lasciano gli utenti nell'incertezza su come controllare la pubblicità dei propri dati.

Fickle — Mancanza di gerarchia (lista di controllo 4.5.1 dell'allegato I)

71. Effetti analoghi a quelli delle ***informazioni contrastanti*** e della ***stimolazione emotiva*** possono verificarsi se la presentazione delle informazioni non segue un sistema interno o una gerarchia. Le informazioni relative alla protezione dei dati presentano una ***mancanza di gerarchia*** quando compaiono più volte e sono presentate in vari modi diversi. È probabile che gli utenti siano confusi da tale ridondanza e non siano in grado di comprendere appieno le modalità con cui i loro dati sono trattati né come esercitare il controllo su di essi. Le informazioni così organizzate sono di difficile comprensione in quanto non è facile accedere al quadro completo. Nei casi come quello descritto nell'esempio seguente, sono violati i requisiti di intelligibilità e facilità di accesso di cui all'articolo 12, paragrafo 1, GDPR.

Example 13: Le informazioni relative ai diritti degli interessati sono disseminate in più punti dell'informativa sulla privacy. Sebbene i diversi diritti degli interessati siano spiegati nella sezione "*Le tue opzioni*", il diritto di presentare un reclamo e l'indirizzo esatto di contatto sono indicati solo dopo diverse sezioni e livelli che riguardano argomenti diversi. L'informativa sulla privacy esclude quindi parzialmente i dati di contatto nelle fasi in cui la loro presenza sarebbe auspicabile e consigliabile.

72. La ***mancanza di gerarchia*** può delinearsi anche quando le informazioni fornite sono strutturate con modalità che rendono agli utenti difficile orientarsi, come dimostra l'esempio che segue.

Example 14: La politica sulla privacy non è suddivisa in sezioni con titoli e contenuti diversi. Consiste di oltre 70 pagine. Non esiste però un menu di navigazione posto a lato o nella parte superiore che consenta agli utenti di accedere facilmente alla sezione che stanno cercando. La spiegazione del termine di propria creazione "*dati di creazione*" è contenuta in una nota a pagina 67.

Left in the dark — Formulazioni o informazioni ambigue (lista di controllo 4.6.3 dell'allegato I)

73. Anche se la scelta delle parole non è manifestamente contraddittoria, possono sorgere problemi dall'uso di termini ambigui e vaghi nel fornire informazioni agli utenti. Di fronte a questo tipo di informazioni gli utenti potrebbero essere incerti sulle modalità di trattamento dei dati o su come esercitare un certo controllo su di essi. Se si può presumere che l'utente medio non comprenderebbe il senso effettivo dell'informazione senza conoscenze specifiche, le condizioni di cui all'articolo 12, paragrafo 1, GDPR non sono soddisfatte. Per analogia, l'uso di ***formulazioni o informazioni ambigue*** può violare il principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR, in quanto le informazioni non possono essere considerate trasparenti, poiché non consentono agli interessati di comprendere il trattamento dei propri dati personali e di esercitare i propri diritti.

Example 15: Un'informativa sulla privacy descrive parte di un trattamento in modo vago e impreciso, come in questa frase: "*I tuoi dati potrebbero essere utilizzati per migliorare i nostri servizi*". Inoltre il diritto di accesso ai dati personali è applicabile al trattamento in forza dell'articolo 15, paragrafo 1, GDPR, ma è menzionato in modo tale che all'utente non è chiaro a cosa possa accedere: *"Puoi visualizzare parte delle tue informazioni nel tuo account e rivedendo ciò che hai pubblicato sulla piattaforma".*

74. Nell'esempio, l'uso del condizionale ("*potrebbero*") lascia l'utente in dubbio sul fatto che i propri dati saranno utilizzati o meno per la finalità del trattamento. Il termine "*servizi*" rischia di essere troppo generico per essere considerato "chiaro". Inoltre non è chiaro in che modo i dati saranno trattati per migliorare i servizi. L'EDPB ricorda che l'uso del modo condizionale o di una formulazione vaga non costituisce un "linguaggio semplice e chiaro" come prescritto dall'articolo 12, paragrafo 1, prima frase, GDPR ed è consentito solo se i titolari del trattamento sono in grado di dimostrare che ciò non pregiudica la correttezza del trattamento[42].

Fickle — Discontinuità linguistica (lista di controllo 4.5.4 dell'allegato I)

75. Quando i servizi online sono offerti e rivolti ai residenti di determinati Stati membri, anche le comunicazioni sulla protezione dei dati dovrebbero essere presentate nelle lingue di tali paesi[43]. In tale contesto è importante che la scelta di una determinata lingua possa essere modificata manualmente e che sia applicata con continuità, senza interruzioni. Se tali criteri non sono soddisfatti, gli interessati si trovano di fronte a una ***discontinuità linguistica*** che impedisce loro di comprendere le informazioni relative alla protezione dei dati. Gli utenti si troveranno di fronte a questo modello di progettazione ingannevole quando le informazioni sulla protezione dei dati non sono fornite in una lingua ufficiale del paese in cui vivono, mentre il servizio è fornito in tale lingua. Se non padroneggiano la lingua in cui sono fornite le informazioni sulla protezione dei dati, gli utenti non saranno in grado di leggerle

[42] Cfr. linee guida sulla trasparenza, punto 12, contenente gli "esempi di pratiche negative", e punto 13.
[43] Cfr. linee guida sulla trasparenza, punto 13 e nota a piè di pagina 15.

facilmente e pertanto non saranno a conoscenza delle modalità di trattamento dei loro dati personali. È importante osservare che la ***discontinuità linguistica*** può confondere gli utenti e creare un ambiente delle impostazioni che non sanno come utilizzare. Come illustrato nelle presenti linee guida, questo modello di progettazione ingannevole può manifestarsi in vari modi.

Example 16:

Variante A: la piattaforma di social media è disponibile in croato come lingua scelta dall'utente (o in spagnolo come lingua del paese in cui si trova l'utente), mentre le informazioni sulla protezione dei dati sono, in tutto o in parte, disponibili solo in inglese.

Variante B: ogni volta che l'utente apre determinate pagine, come la pagina di assistenza, queste passano automaticamente alla lingua del paese in cui si trova l'utente, anche se in precedenza è stata selezionata una lingua diversa.

76. La variante A illustra il caso in cui non sono disponibili informazioni nella lingua presumibilmente conosciuta dall'interessato. Ciò significa che questi non è in grado di leggere le informazioni e, per analogia, non può comprendere come vengono trattati i suoi dati personali. Le informazioni non possono essere considerate intelligibili ai sensi dell'articolo 12, paragrafo 1, GDPR. A causa della mancanza di informazioni sulla protezione dei dati fornite nella lingua che è in grado di comprendere, non si può ritenere che l'interessato abbia ricevuto le informazioni prescritte rispettivamente dagli articoli 13 e 14 GDPR.

77. La variante B descrive un caso in cui le pagine informative sulla protezione dei dati sono presentate per impostazione predefinita nella lingua del paese di residenza dell'utente, nonostante la sua chiara scelta linguistica. L'utente deve pertanto reimpostare la propria preferenza linguistica ogni volta che accede a una pagina informativa sulla protezione dei dati. Questa può essere considerata una pratica scorretta nei confronti dell'interessato e potrebbe comportare la violazione del principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR.

ii. Modelli basati sull'interfaccia

78. In alcuni casi i fornitori di social media si avvalgono di pratiche specifiche per la presentazione delle proprie impostazioni in materia di protezione dei dati. Durante il processo di iscrizione, agli utenti sono fornite molte informazioni e diverse impostazioni relative alla protezione dei dati. Per garantire che gli utenti possano riuscire a ritornarvi per modificarle in qualsiasi momento durante l'utilizzo della piattaforma, le impostazioni dovrebbero essere facilmente accessibili e associate a informazioni pertinenti che consentano agli utenti di prendere una decisione informata. L'elemento della "facile accessibilità" implica che gli interessati non siano costretti a cercare le informazioni. Per quanto riguarda le politiche sulla privacy, il Gruppo di lavoro articolo 29 ha già rilevato che sistemi di posizionamento o combinazioni di colori che rendono un testo o un link meno visibili o difficili da trovare su una pagina web non sono considerati conformi al criterio della facile accessibilità[44].

[44] Linee guida sulla trasparenza, punto 11.

Overloading — Privacy intricata (lista di controllo 4.1.2 dell'allegato I)

79. Conformemente alle linee guida sulla trasparenza, l'informativa sulla privacy dovrebbe essere facilmente accessibile, vale a dire tramite un solo click all'interno del sito web[45]. Il ricorso al metodo dell'approccio a più livelli può aiutare a presentare l'informativa sulla privacy in modo più chiaro ai sensi dell'articolo 12, paragrafo 1, GDPR[46]. Non si dovrebbe tuttavia rendere immotivatamente difficoltoso l'esercizio di funzioni o diritti importanti fornendo una politica sulla privacy complessa, articolata su innumerevoli livelli che darebbero luogo al modello ingannevole della ***privacy intricata***. Tale modello si ha quando un'informazione o un controllo riguardanti la protezione dei dati è particolarmente difficile da trovare, in quanto gli utenti devono navigare attraverso molte pagine senza riuscire a ottenere una panoramica completa ed esaustiva. È pertanto probabile che gli utenti non notino le informazioni/l'impostazione pertinenti o rinuncino alla loro ricerca. Il sistema di presentazione su più livelli è inteso a facilitare la leggibilità e a fornire informazioni sulle modalità di esercizio dei propri diritti da parte degli interessati, non ad aumentare le difficoltà. È fondamentale garantire che gli utenti possano seguire facilmente le spiegazioni.

80. A tale riguardo, la soluzione migliore per gli utenti non consiste nell'adozione di un metodo unico valido per tutti, ma dipende da numerosi criteri, come il tipo di utenti della piattaforma o il tipo generale di progettazione dell'applicazione. Ove possibile, per valutare l'efficacia del sistema a più livelli adottato si dovrebbe testarne l'efficacia ottenendo il feedback degli utenti. Per questo motivo non è possibile quantificare uno specifico numero massimo di livelli di informazione ammissibili. Occorre pertanto stabilire caso per caso l'eventuale utilizzo di un numero eccessivo di livelli e quindi la presenza di modelli di progettazione ingannevoli. Tuttavia, quanto maggiore è il numero di livelli, tanto più è presumibile che gli utenti saranno scoraggiati o indotti in errore. Un numero elevato di livelli sarà appropriato solo in casi particolari in cui risulta difficile fornire in modo esaustivo informazioni complesse. Allo stesso tempo, l'approccio a più livelli non può essere utilizzato impropriamente per nascondere informazioni nei livelli secondari o aggiungendo livelli superflui.

81. Questo aspetto deve essere però valutato in modo diverso quando si tratta dell'esercizio dei diritti degli utenti. Il GDPR impone che l'esercizio di tali diritti sia sempre garantito. Tale quadro disciplina la presentazione delle informazioni sulle funzioni correlate e l'esercizio dei diritti. Quando gli utenti desiderano esercitare i propri diritti, il numero di passaggi dovrebbe essere il minore possibile. Di conseguenza, gli utenti dovrebbero arrivare alla funzione che consente loro di esercitare i propri diritti nel modo più diretto possibile. Nella maggior parte dei casi, il fatto di dover navigare in un numero elevato di livelli di informazione prima di trovare le funzioni tramite cui esercitare effettivamente i propri diritti potrebbe dissuadere gli utenti dall'esercizio dei medesimi. Se sono previsti molti passaggi, il fornitore di social media dovrebbe essere in grado di dimostrare il vantaggio che ciò comporta per gli utenti in quanto interessati ai sensi del GDPR. Oltre alla spiegazione dei diritti dell'interessato nell'informativa sulla privacy, prevista dall'articolo 13, paragrafo 2, lettere b), c) e d), GDPR, l'esercizio dei diritti dovrebbe essere accessibile indipendentemente da tali informazioni. Ad esempio gli utenti dovrebbero poter esercitare i diritti degli interessati anche attraverso il menu della piattaforma.

> **Example 17:** Il fornitore di social media mette a disposizione sulla propria piattaforma un documento denominato "*consigli utili*" che contiene anche informazioni importanti sull'esercizio dei diritti dell'interessato. Tuttavia la politica sulla privacy non contiene alcun link o altro accenno al documento citato, ma indica che maggiori informazioni sono disponibili

[45] Cfr. linee guida sulla trasparenza, esempio al punto 11.

[46] Per maggiori dettagli sull'approccio a più livelli in un ambiente digitale, cfr. linee guida sulla trasparenza, punti da 35 a 37.

nella sezione del sito web dedicata a domande e risposte. Gli utenti che si aspettano informazioni sui loro diritti nella politica sulla privacy non vi troveranno quindi tali spiegazioni e dovranno continuare la navigazione per cercarle nella sezione dedicata a domande e risposte.

82. Quello descritto è un chiaro esempio di modello di ***privacy intricata***, che, in violazione dell'articolo 12, paragrafo 2, GDPR, rende l'accesso a maggiori informazioni riguardanti i diritti dell'interessato e, in particolare, le modalità di esercizio di tali diritti più difficile del dovuto. Inoltre una politica sulla privacy incompleta costituisce anche una violazione rispettivamente dell'articolo 13, paragrafo 2, lettere b), c) e d), e dell'articolo 14, paragrafo 2, lettere c), d) ed e), GDPR. Infatti le informazioni più dettagliate o il mezzo diretto per esercitare i diritti potevano essere resi accessibili con un solo clic nel punto della politica sulla privacy in cui sono menzionati, mentre, nell'esempio fornito, per trovare il documento "*consigli utili*" gli utenti devono aprire e leggere la pagina delle domande e risposte.

83. È importante osservare che gli effetti derivanti dalla presenza di un numero eccessivo di livelli[47] possono essere persino più gravi quando sono utilizzati non solo più dispositivi, ma anche diverse applicazioni fornite dalla stessa piattaforma di social media, come ad esempio speciali applicazioni di messaggistica. Gli utenti che utilizzano questo tipo di applicazioni secondarie incontrerebbero maggiori ostacoli e difficoltà se dovessero aprire la versione per browser o l'applicazione principale per ottenere informazioni relative alla protezione dei dati. In una situazione del genere, in cui non sono coinvolti soltanto più dispositivi ma anche più applicazioni, le informazioni pertinenti devono sempre essere direttamente accessibili, indipendentemente dal modo in cui gli utenti utilizzano la piattaforma.

Obstructing — Punto morto (lista di controllo 4.4.1 dell'allegato I)

84. Si può configurare una violazione degli obblighi normativi anche quando l'accesso alle informazioni sulla protezione dei dati previste dal GDPR è reso possibile solo mediante ulteriori azioni, ad esempio un clic su un link o su un pulsante. In particolare, non può essere considerata corretta ai sensi dell'articolo 5, paragrafo 1, lettera a), GDPR una navigazione fuorviante o una progettazione incoerente dell'interfaccia che conduce a funzionalità inutili, in quanto induce in errore gli utenti quando cercano di ottenere informazioni o di impostare le proprie preferenze in materia di protezione dei dati. Devono pertanto essere assolutamente evitati ***punti morti*** in cui gli utenti siano abbandonati senza alcuna funzione a disposizione per esercitare i propri diritti, in diretta violazione dell'articolo 12, paragrafo 2, GDPR, che stabilisce che il titolare del trattamento deve agevolare l'esercizio dei diritti dell'interessato.

Example 18: Nella politica sulla privacy di un fornitore di social media sono presenti numerosi collegamenti ipertestuali a pagine contenenti ulteriori informazioni su argomenti specifici. Tuttavia in diverse parti del documento si dichiara solo in modo generico che è possibile accedere a ulteriori informazioni, senza indicare in quali sedi e con quali modalità.

85. La politica sulla privacy è generalmente considerata il documento che raccoglie tutte le informazioni relative agli aspetti legati alla protezione dei dati conformemente agli obblighi di cui agli articoli 12, 13 e 14 GDPR. È pertanto necessario garantire anche il reindirizzamento verso tutti i punti pertinenti della piattaforma di social media per consentire agli utenti di controllare i propri dati o di esercitare i propri diritti. Nell'esempio 18 ciò è attuato solo in parte, in quanto i link a ulteriori informazioni sono forniti per alcuni elementi, ma non per altri. Per questi motivi, il modello del ***punto morto*** può comportare

[47] Cfr. sopra, punti 81 e 82.

una violazione dell'articolo 12, paragrafo 1, GDPR, rendendo difficile l'accesso ad alcune informazioni sulla protezione dei dati, o dell'articolo 12, paragrafo 2, GDPR, non agevolando l'esercizio dei diritti.

d. **Migliori prassi**

Menu di navigazione "*sticky*" (fisso): durante la consultazione di una pagina relativa alla protezione dei dati, l'indice può rimanere costantemente visibile sullo schermo, in modo da consentire agli utenti di individuare la propria posizione nella pagina in ogni momento e di spostarsi rapidamente nel contenuto grazie a link di ancoraggio.

Inizio pagina: inserire in fondo alla finestra un pulsante che consente di tornare all'inizio della pagina o un elemento costantemente visibile sullo schermo che consente di spostarsi facilmente all'interno di una pagina.

Scorciatoie: per la definizione cfr. il caso d'uso n. 1 (pag. 22) (*ad esempio, nella politica sulla privacy, fornire, per ciascuna informazione sulla protezione dei dati, link che reindirizzano direttamente alle corrispondenti pagine della piattaforma di social media relative alla protezione dei dati*).

Informazioni di contatto: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Indicazioni per contattare l'autorità di controllo: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Panoramica della politica sulla privacy: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Individuazione e confronto delle modifiche: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Formulazioni coerenti: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Fornitura di definizioni: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Uso di esempi: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Caso d'uso n. 2b: fornire all'interessato informazioni sulla contitolarità del trattamento, articolo 26, paragrafo 2, GDPR

a. Descrizione del contesto e disposizioni giuridiche pertinenti

86. La seconda frase dell'articolo 26, paragrafo 2, GDPR prevede ulteriori disposizioni in materia di trasparenza nel caso specifico di contitolarità del trattamento[48], che garantiscono che il contenuto essenziale dell'accordo di contitolarità del trattamento sia messo a disposizione dell'interessato[49]. Nelle sue linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, l'EDPB raccomanda che tale contenuto essenziale dell'accordo riguardi almeno tutti gli elementi delle informazioni di cui agli articoli 13 e 14 GDPR che dovrebbero già essere accessibili agli interessati e, per ciascuno di tali elementi, di specificare il contitolare del trattamento responsabile

[48] Per la definizione di contitolarità del trattamento, cfr. l'articolo 4, punto 7), in combinato disposto con l'articolo 26, paragrafo 1, prima frase, GDPR nonché le linee guida 07/2020 dell'EDPB sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, adottate il 7 luglio 2021, versione 2.1, punti 46-49, disponibili all'indirizzo https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_it.pdf.

[49] Cfr. EDPB, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, punto 179.

di garantirne il rispetto[50]. Il contenuto essenziale dell'accordo deve comprendere anche il punto di contatto, se designato. Spetta ai contitolari del trattamento decidere il modo più efficace per mettere a disposizione degli interessati il contenuto essenziale dell'accordo[51].

b. Modelli di progettazione ingannevoli

Example 19: Per quanto riguarda i modelli di progettazione ingannevoli, la sfida per i titolari del trattamento in questa costellazione consiste nell'integrare tali informazioni nel sistema online in modo che possano essere facilmente recepite e non perdano chiarezza e comprensibilità, anche se l'articolo 12, paragrafo 1, prima frase, GDPR non fa direttamente riferimento all'articolo 26, paragrafo 2, seconda frase, GDPR. Tuttavia, in virtù dei principi di protezione dei dati quali la correttezza, la trasparenza e la responsabilizzazione di cui all'articolo 5, paragrafo 1, lettera a), e all'articolo 5, paragrafo 2, GDPR, obblighi comparabili sorgono anche nel caso di contitolarità del trattamento. Quando forniscono informazioni sul contenuto essenziale dell'accordo in un'informativa sulla privacy, i contitolari del trattamento devono anche farlo in modo chiaro e trasparente. Pertanto il trattamento non può più essere considerato corretto se le relative informazioni risultano di difficile comprensione perché non sono forniti i link o le informazioni sono distribuite in diverse sezioni dell'informativa. Il modello di progettazione ingannevole della ***privacy intricata***[52] potrebbe confondere ancora di più di quanto non faccia di norma un'informativa sulla privacy, in quanto gli utenti possono aspettarsi che le informazioni di cui all'articolo 26, paragrafo 2, seconda frase, GDPR siano fornite in un'unica sezione. Un fornitore di social media fa sempre riferimento ai "*dati di creazione*" nell'ambito della politica sulla privacy e non utilizza il termine "dati personali". Solo a pagina 90 dell'informativa sulla privacy a più livelli è spiegato che "*i dati di creazione potrebbero includere dati personali degli utenti*". Anche nel contenuto essenziale dell'accordo relativo al contitolare del trattamento fornito agli interessati si utilizza il termine "dati di creazione", senza alcuna spiegazione. Nella politica sulla privacy dell'altro contitolare del trattamento (B) è fornita una definizione di dati personali. Tuttavia, nella sezione relativa alla contitolarità del trattamento con il fornitore di social media, B inserisce solo un link all'accordo fornito dal fornitore di social media, senza altre spiegazioni.

87. Le spiegazioni di cui all'articolo 26, paragrafo 2, frase 2, GDPR sono più difficili da comprendere se diventano incoerenti. Questo effetto di incoerenza è amplificato quando le piattaforme di social media utilizzano una terminologia di propria creazione che gli utenti solitamente non associano al trattamento dei dati personali, come illustrato nell'esempio 19. Nell'esempio, entrambi i contitolari del trattamento violano l'articolo 26, paragrafo 2, seconda frase, nonché l'articolo 5, paragrafo 1, lettera a), GDPR, in quanto le informazioni fornite sulla contitolarità del trattamento sono poco chiare e pertanto risultano non trasparenti per l'interessato.

[50] Cfr. EDPB, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, punto 180, anche per la frase successiva.
[51] EDPB, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, punto 181.
[52] Cfr. il caso d'uso n. 2a, esempio 17 delle presenti linee guida.

Caso d'uso n. 2c: comunicazione di una violazione dei dati personali all'interessato

a. Descrizione del contesto e disposizioni giuridiche pertinenti

88. Per poter individuare e porre rimedio a una violazione dei dati, il titolare del trattamento deve essere in grado di riconoscerla[53]. Ai sensi dell'articolo 4, punto 12), GDPR, per "violazione dei dati personali" si intende una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Per quanto riguarda i titolari del trattamento sui social media, le violazioni dei dati possono verificarsi in diversi modi. Ad esempio, se l'autore di un attacco riesce ad accedere ai dati personali e ai messaggi della chat degli utenti. Oppure, a causa di un errore di programmazione, un'app potrebbe accedere a dati personali con modalità che vanno oltre quanto autorizzato dagli utenti. Un altro esempio potrebbe essere rappresentato dal fatto che gli utenti condividono immagini in virtù dell'impostazione "condivido con i miei migliori amici", ma le loro immagini sono messe a disposizione di un gruppo più ampio di persone. Come ultimo esempio, un bug potrebbe consentire a una piattaforma di social media basata su video in tempo reale di condividere ulteriori streaming di contenuti, nonostante gli utenti avessero precedentemente premuto un pulsante per interrompere la registrazione.

89. In caso di violazione dei dati personali, il titolare del trattamento ne dà notifica in ogni caso all'autorità di controllo competente a norma dell'articolo 33 GDPR, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve, di norma, comunicare la violazione anche all'interessato ai sensi dell'articolo 34, paragrafi 1 e 2, GDPR. In tal caso il titolare del trattamento deve informare l'interessato senza ingiustificato ritardo. Tale comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali, in quanto si applica anche l'articolo 12 GDPR. Inoltre essa deve contenere almeno informazioni e misure quali (cfr. anche articolo 33, paragrafo 3, lettere da b) a d), in combinato disposto con l'articolo 34, paragrafo 2, GDPR):

- il nome e i dati di contatto del responsabile della protezione dei dati, se applicabile, o di un altro punto di contatto presso cui ottenere più informazioni;
- una descrizione delle probabili conseguenze della violazione dei dati personali; e
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi[54].

90. Anche tali comunicazioni di violazione dei dati ai sensi dell'articolo 34 GDPR possono contenere modelli di progettazione ingannevoli. Ad esempio, se il rispettivo titolare del trattamento fornisce agli interessati tutte le informazioni necessarie per informarli in merito alla portata della violazione dei dati, ma fornisce loro anche informazioni non specifiche e irrilevanti e che riguardano implicazioni e misure precauzionali che il titolare del trattamento ha adottato o suggerisce di adottare. Tali informazioni parzialmente irrilevanti possono essere fuorvianti e gli utenti interessati dalla violazione

[53] Cfr. anche EDPB, *Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*, adottate il 14 dicembre 2021, versione 2.0, punto 4, disponibili all'indirizzo: https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_it.pdf.

[54] Gruppo di lavoro articolo 29 per la protezione dei dati, *Linee guida sulla notifica della violazione dei dati personali ai sensi del regolamento (UE) 2016/679*, approvate dall'EDPB, pag. 20; https://ec.europa.eu/newsroom/article29/items/61205n2/en.

potrebbero non comprendere appieno le implicazioni della violazione stessa o sottovalutarne gli effetti (potenziali).

b. Modelli di progettazione ingannevoli

91. Per citare alcuni esempi negativi, le pratiche scorrette consistenti nelle notifiche di violazione dei dati contrarie all'articolo 34 GDPR in combinato disposto con l'articolo 12 GDPR potrebbero verificarsi nei modi seguenti:

i. Modelli basati sui contenuti

Left in the dark — Informazioni contrastanti (lista di controllo 4.6.2 dell'allegato I)

> **Example 20:**
>
> • Il titolare del trattamento fa riferimento unicamente ad azioni di terzi, al fatto che la violazione dei dati è stata generata da un terzo (ad esempio un responsabile del trattamento) e che pertanto non si è verificata alcuna violazione della sicurezza. Il titolare del trattamento sottolinea inoltre alcune buone pratiche che non hanno nulla a che vedere con la violazione verificatisi.
>
> • Il titolare del trattamento dichiara la gravità della violazione in relazione a se stesso o a un responsabile del trattamento, piuttosto che in relazione all'interessato.

Left in the dark — Formulazioni o informazioni ambigue (lista di controllo 4.6.3 dell'allegato I)

92. Per quanto riguarda il linguaggio della comunicazione della violazione all'interessato, è fondamentale che i titolari del trattamento tengano presente che la maggior parte dei destinatari non avrà familiarità con il linguaggio specifico, talvolta tecnico o giuridico, legato alla protezione dei dati.

> **Example 21:** Una violazione dei dati su una piattaforma di social media ha reso accidentalmente accessibili a utenti non autorizzati alcune serie di dati sanitari. Il fornitore di social media si limita a informare gli utenti del fatto che alcune "*categorie particolari di dati personali*" sono state accidentalmente rese pubbliche.

93. Si tratta di una ***formulazione ambigua***, in quanto gli utenti medi non comprendono l'espressione "*categorie particolari di dati personali*" e pertanto non sanno che i loro dati sanitari sono stati divulgati. Ciò è dovuto al fatto che l'accezione del termine "particolare" nel linguaggio generale è molto diversa da quella propria del linguaggio specifico legato al GDPR. L'utente medio non sa che, a norma dell'articolo 9, paragrafo 1, GDPR, le *"categorie particolari di dati personali"* riguardano dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, oppure dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Pertanto in questo contesto la formulazione "*categorie particolari di dati personali*" costituisce un modello di progettazione ingannevole, in quanto induce in errore gli utenti non essendo accompagnata da ulteriori spiegazioni. Si tratta di un esempio di situazione in cui un titolare del trattamento cerca di informare gli interessati in merito alla violazione, ma non adempie pienamente all'obbligo di comunicare la violazione dei dati a norma dell'articolo 34 GDPR, in quanto la gravità dell'incidente sarà sottovalutata dal lettore medio. Inoltre le scarne informazioni contenute nell'esempio non sono

comprensibili, come invece prescritto dall'articolo 34 in combinato disposto con l'articolo 12, paragrafo 1, prima frase, GDPR.

94. Un altro esempio di ***formulazione ambigua*** è riportato di seguito.

> **Example 22:** Nell'indicare le categorie di dati personali interessati, il titolare del trattamento fornisce soltanto informazioni generiche, ad esempio fa riferimento ai documenti presentati dagli utenti, senza specificare quali categorie di dati personali siano incluse in tali documenti e quanto siano sensibili.

95. È importante notare che il modello di progettazione ingannevole in questione può emergere in tutti gli elementi della notifica di violazione dei dati. Mentre i due esempi sopra citati fanno riferimento a una formulazione poco chiara delle categorie dei dati interessate, l'esempio successivo mostra che altrettanto poco chiara potrebbe essere la categoria degli interessati.

> **Example 23:** nel segnalare la violazione, il titolare del trattamento non specifica adeguatamente la categoria degli interessati coinvolti; ad esempio indica solo che gli interessati erano studenti, ma non specifica se si tratti di minori o di gruppi vulnerabili.

96. Infine la gravità dell'incidente può essere sottovalutata anche quando sono fornite ***informazioni ambigue***, come nell'esempio illustrato di seguito.

> **Example 24:** Quando notifica la violazione all'autorità di controllo e all'interessato, il titolare del trattamento dichiara che i dati personali sono stati resi pubblici tramite altre fonti. L'interessato ritiene pertanto che non vi sia stata alcuna violazione della sicurezza.

ii. Modelli basati sull'interfaccia

97. Anche esempi negativi di notifiche di violazione dei dati contrarie all'articolo 34 del GDPR in combinato disposto con l'articolo 12 GDPR possono costituire modelli di progettazione ingannevoli basati sull'interfaccia, come illustrato di seguito:

Skipping — Diversivo (lista di controllo 4.2.2 dell'allegato I)

> **Example 25:**
>
> • Il titolare del trattamento effettua la comunicazione utilizzando testi che contengono molte informazioni non pertinenti e in cui si omettono i dettagli pertinenti.
>
> • Nei casi di violazioni della sicurezza che incidono sulle credenziali di accesso e su altri tipi di dati, il titolare del trattamento dichiara che i dati sono cifrati o sono stati sottoposti ad *hashing*, mentre ciò avviene solo per le password.

98. In questo caso, anche se la comunicazione contiene le informazioni pertinenti, è probabile che gli interessati ne siano distolti a causa di un sovraccarico di informazioni irrilevanti.

c. Migliori prassi

> **Notifiche**: le notifiche possono essere utilizzate per sensibilizzare gli utenti su aspetti, cambiamenti o rischi connessi al trattamento dei dati personali (ad esempio *in caso di violazione dei dati*). L'attuazione delle notifiche può avvenire in vari modi, ad esempio attraverso messaggi di posta in arrivo, finestre pop-in, banner fissi nella parte superiore della pagina web ecc.

Spiegazione delle conseguenze: se gli utenti desiderano attivare o disattivare un controllo della protezione dei dati o prestare o revocare il proprio consenso, informarli in modo neutro sulle conseguenze di tale azione.

Scorciatoie: per la definizione cfr. il caso d'uso n. 1 (pag. 22) (*ad esempio, fornire agli utenti un link per reimpostare la password*).

Formulazioni coerenti: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Fornitura di definizioni: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Uso di esempi: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

3.3 Rimanere protetti sui social media

Caso d'uso n. 3a: la gestione del consenso nell'uso di una piattaforma di social media

a. Descrizione del contesto e disposizioni giuridiche pertinenti

99. Gli utenti delle piattaforme di social media devono fornire il proprio consenso durante le diverse fasi delle attività di trattamento dei dati, ad esempio prima di ricevere pubblicità personalizzata. Come già indicato nelle linee guida dell'EDPB sul *targeting* degli utenti dei social media, il consenso può costituire una base giuridica adeguata solamente se all'interessato sono assicurati il controllo e una scelta effettiva55. Inoltre, a norma dell'articolo 4, punto 11), GDPR, il consenso deve essere specifico, informato e inequivocabile56. È importante sottolineare che i requisiti per un consenso valido ai sensi del GDPR non costituiscono un obbligo aggiuntivo, ma sono condizioni preliminari per il trattamento lecito dei dati personali degli utenti. Inoltre, per quanto riguarda il marketing online o i metodi di tracciamento online, si applica la direttiva 2002/58/CE (direttiva e-privacy). Tuttavia i prerequisiti per un consenso valido ai sensi della direttiva e-privacy sono identici alle disposizioni relative al consenso contenute nel GDPR57.

100. Tenuto conto del principio di responsabilizzazione di cui all'articolo 5, paragrafo 2, GDPR, nonché della necessità che il titolare del trattamento sia in grado di dimostrare che gli interessati hanno prestato il proprio consenso al trattamento dei propri dati personali a norma dell'articolo 7, paragrafo 1, GDPR, è fondamentale che il fornitore di social media possa dimostrare di aver adeguatamente ottenuto il consenso degli utenti. Si tratta di una condizione che potrebbe essere difficile da dimostrare, ad esempio se si ritiene che gli utenti diano il consenso accettando i cookie. Inoltre gli interessati potrebbero non essere sempre consapevoli del fatto che stanno dando il loro consenso mentre cliccano velocemente su un pulsante evidenziato o su opzioni preimpostate. Tuttavia, come sottolinea l'articolo 7, paragrafo 1, GDPR, l'onere della prova del consenso liberamente espresso degli utenti è a carico del titolare del trattamento.

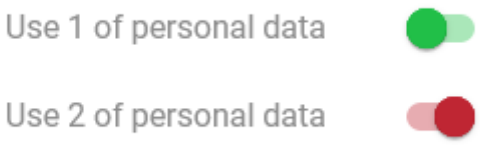
[55] Linee guida 08/2020 sul *targeting* degli utenti di social media, punto 51.
[56] Cfr. anche i precedenti punti da 25 a 29.
[57] Cfr. l'articolo 2, lettera f), della direttiva 2002/58/CE e EDPB, parere 5/2019 sull'interazione tra la direttiva e-privacy e il regolamento generale sulla protezione dei dati, in particolare per quanto concerne competenze, compiti e poteri dell'autorità di protezione dei dati, adottato il 12 marzo 2019, punto 14, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_it.

b. Modelli di progettazione ingannevoli

i. Modelli basati sui contenuti

101. Oltre ai modelli basati sui contenuti già illustrati in precedenza che potrebbero applicarsi alle informazioni relative a una richiesta di consenso[58], è possibile evidenziare altri due modelli di progettazione ingannevoli basati sui contenuti in relazione al consenso.

Informazioni contrastanti — Left in the dark (lista di controllo 4.6.2 dell'allegato I)

> **Example 26:** L'interfaccia utilizza un selettore a levetta per consentire all'utente di prestare o revocare il consenso. Tuttavia il meccanismo della levetta non consente di capire con certezza su quale posizione il selettore sia impostato e se l'utente abbia prestato o meno il consenso. Infatti non vi è corrispondenza tra la posizione della levetta e il colore del selettore. Se la levetta è sul lato destro, solitamente associato all'attivazione di una funzione ("acceso"), il colore del selettore è il rosso, che di solito indica una funzione disattivata. Viceversa, quando la levetta si trova sul lato sinistro, posizione che di norma indica una funzione disattivata, il colore dello sfondo è il verde, solitamente associato a un'opzione attiva.
>
> 
>

102. Fornire ***informazioni contrastanti*** al momento dell'ottenimento del consenso rende l'informativa poco chiara e incomprensibile. L'esempio precedente illustra un caso in cui le informazioni visive sono ambigue: guardando le levette gli utenti non avranno infatti la certezza di avere dato o meno il consenso. Quando i segnalatori visivi sono così confusi o sono presentati in altri colori che sembrano in contraddizione con l'impostazione effettiva — l'esempio 26 rappresenta solo un caso di selettori che ingenerano confusione — il consenso non può essere considerato fornito in modo inequivocabile, ai sensi dell'articolo 7, paragrafo 2, GDPR, in combinato disposto con l'articolo 4, punto 11), GDPR. Le ***informazioni contrastanti*** possono essere fornite anche con mezzi testuali, come illustrato di seguito.

> **Example 27:** Il fornitore di social media fornisce informazioni contraddittorie agli utenti: nelle informazioni si afferma innanzitutto che i contatti non sono importati senza il consenso, ma al tempo stesso una finestra informativa pop-up spiega in che modo i contatti saranno comunque importati.

Obstructing — Azione ingannevole (lista di controllo 4.4.3 dell'allegato I)

103. Oltre a fornire ***informazioni contrastanti***, i titolari del trattamento possono elaborare informazioni che inducono in errore gli utenti in quanto non corrispondono a quanto essi si aspettano. Si ha un'***azione ingannevole*** quando una discrepanza tra le informazioni e le azioni a disposizione degli utenti li induce

[58]Cfr. il caso d'uso n. 1, punti da 32 a 49, o numeri di esempio UC1 elencati nell'allegato.

a compiere un'operazione non voluta. La differenza tra ciò che gli utenti si aspettano e ciò che ottengono rischia di dissuaderli dal proseguire.

> **Example 28:** L'utente consulta il proprio feed sui social media. Nel mentre, gli appaiono annunci pubblicitari. Intrigato da uno di essi e curioso di sapere perché gli compaia, clicca sul simbolo "?" visibile nell'angolo inferiore destro dell'annuncio. Si apre una finestra pop-in che spiega perché l'utente veda la pubblicità in questione ed elenca i criteri di *targeting*. Informa inoltre l'utente che può revocare il proprio consenso alla pubblicità mirata e fornisce un link a tal fine. Cliccando su tale link l'utente è reindirizzato in un sito web completamente diverso che fornisce spiegazioni generali sul consenso e su come gestirlo.

104. Quello descritto sopra è un caso emblematico di contenuti che non rispondono alle aspettative dell'utente. Infatti, quando clicca sul link, l'utente si aspetta di essere reindirizzato a una pagina che gli consenta di revocare direttamente il proprio consenso. Si apre invece una pagina che non gli offre tale possibilità né gli indica le modalità specifiche per revocare il proprio consenso sulla piattaforma di social media. Il divario tra quello che l'utente si aspetta di trovare e quello che effettivamente trova rischia di confonderlo e di disorientarlo su come procedere. Nel peggiore dei casi, l'utente potrebbe ritenere di non avere la possibilità di revocare il proprio consenso. Tale ***azione ingannevole*** non può essere considerata trasparente, come invece prescritto dall'articolo 12, paragrafo 1, GDPR. Inoltre, mettendo a confronto le modalità per la revoca con quelle per l'ottenimento del consenso, tale pratica potrebbe violare l'articolo 7, paragrafo 3, GDPR, qualora revocare il consenso si riveli più difficile di concederlo.

105. Quando i fornitori di social media informano gli utenti che un'azione da parte di questi ultimi può avere una certa conseguenza e l'azione porta di fatto a un risultato diverso, ciò costituisce un'***azione ingannevole***, come illustrato nell'esempio successivo.

> **Example 29:** Nella parte dell'account di social media dedicata alla condivisione di pensieri, immagini ecc., l'utente è invitato a indicare se desidera condividere tali contenuti una volta che li ha digitati o caricati. L'utente può scegliere tra il pulsante "*Sì, grazie*" e il pulsante "*No, grazie*" Tuttavia, dopo che l'utente ha deciso di non condividere i contenuti con altri cliccando sul secondo pulsante, il contenuto è pubblicato sul suo account di social media.

106. Come nell'esempio precedente, le informazioni non sono trasparenti e privano l'utente della possibilità di scegliere. Anche se l'utente potrebbe rendersi subito conto della pubblicazione e cancellarla, i dati, malgrado il suo rifiuto, sono stati trattati e resi visibili ad altri. Un caso ancora più grave è quello in cui l'utente non può accorgersi del trattamento oppure può accorgersene soltanto con difficoltà o se conosce le tecnologie informatiche, in quanto questo avviene in secondo piano nella piattaforma di social media.

ii. Modelli basati sull'interfaccia

107. Oltre ai due modelli di progettazione ingannevoli di cui sopra, in questo caso d'uso sono rilevanti soprattutto i modelli basati sull'interfaccia.

Skipping — Diversivo (lista di controllo 4.2.2 dell'allegato I)

108. Quando un'azione o un'informazione relativa alla protezione dei dati è messa in concorrenza con un altro elemento connesso o meno alla protezione dei dati, è probabile che gli utenti che scelgono quest'ultima opzione finiscano per trascurare l'altra, anche se questa costituiva il loro primo obiettivo. Si tratta di un modello di ***diversivo*** che deve essere valutato caso per caso.

> **Example 30:** Un cookie banner della piattaforma di social media recita: "Per biscotti (*cookie*) deliziosi bastano burro, zucchero e farina. Consulta la nostra ricetta preferita qui [link]. Anche noi usiamo i cookie. Per saperne di più leggi la nostra politica in materia di cookie [link].", insieme al pulsante "okay".

109. L'umorismo non dovrebbe essere utilizzato per travisare i rischi potenziali e inficiare le informazioni effettive. In questo esempio l'utente potrebbe essere tentato di cliccare solo sul primo link, leggere la ricetta dei biscotti e poi cliccare sul pulsante "*okay*". Oltre a non fornire agli utenti un mezzo per negare il consenso, questo esempio illustra un caso in cui il consenso potrebbe non essere adeguatamente informato. Infatti, cliccando sul pulsante "*okay*", l'utente potrebbe credere di ignorare un messaggio spiritoso sui cookie, intesi come dolcetti, senza rendersi conto del significato tecnico del termine *cookie*. Questo caso non costituirebbe un consenso informato ai sensi dell'articolo 7, paragrafo 2, del GDPR, in combinato disposto con l'articolo 4, punto 11), GDPR.

110. L'articolo 7, paragrafo 2, GDPR stabilisce inoltre che una richiesta di consenso dovrebbe essere chiaramente distinguibile da altre materie. È pertanto necessario che le informazioni sulla protezione dei dati non siano messe in ombra da altri contesti. Nell'esempio esaminato, il gioco di parole basato sulla duplice accezione del termine inglese "cookie" può far sì che il contesto della pasticceria oscuri quello della protezione dei dati. Affinché le informazioni siano chiaramente distinguibili, le informazioni pertinenti che consentono agli utenti di fornire un consenso valido dovrebbero essere in primo piano, non rese ***poco visibili***, e non mescolate con altri argomenti o significati. Le informazioni sulla protezione dei dati non dovrebbero essere confuse con altri tipi di contenuti. In caso contrario l'attenzione degli utenti potrebbe essere distolta dalle reali implicazioni del trattamento dei loro dati personali. Nell'attuazione di tali prerequisiti è necessario lasciare ai progettisti un certo margine di manovra per rendere le informazioni attraenti.

Obstructing — Punto morto (lista di controllo 4.4.1 dell'allegato I)

111. La confusione o la distrazione non sono l'unico effetto possibile derivante da modelli di progettazione ingannevoli per quanto riguarda il consenso. In particolare, il modello di ***punto morto*** può interferire in vari modi con le condizioni per il consenso di cui all'articolo 7, in combinato disposto con l'articolo 4, punto 11), GDPR.

> **Example 31:** L'utente desidera gestire le autorizzazioni concesse alla piattaforma dei social media sulla base del consenso. Deve trovare una pagina delle impostazioni relativa a tale funzione e intende disabilitare la condivisione dei propri dati personali per finalità di ricerca. Quando clicca sulla casella per togliere la spunta, non accade nulla a livello di interfaccia e ha l'impressione che il consenso non possa essere revocato.

112. In questo esempio specifico il modello di ***punto morto*** potrebbe violare l'articolo 7, paragrafo 3, GDPR, in quanto all'utente non sembra essere data la possibilità di revocare il proprio consenso al trattamento dei dati personali per finalità di ricerca, poiché il mezzo per farlo non sembra funzionare.

Se l'azione dell'utente non è correttamente registrata all'interno del sistema, si può configurare una violazione dell'articolo 7, paragrafo 3, GDPR. Se la scelta è effettivamente registrata nel sistema, il fatto che l'interfaccia non rifletta l'azione dell'utente potrebbe essere considerato non conforme al principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR. Quando sembra offrire i mezzi per gestire correttamente il consenso, consentendo agli utenti di dare il proprio consenso o di revocarlo, ma non produce alcun effetto visivo quando questi interagiscono con essa, un'interfaccia risulta fuorviante e crea confusione e perfino frustrazione negli utenti. Tale discrepanza tra lo stato in cui si trova il sistema e le informazioni trasmesse dall'interfaccia dovrebbe essere evitata, in quanto in generale può ostacolare il controllo dei propri dati personali da parte degli utenti.

113. Molte attività di trattamento coinvolgono più parti, ossia un altro (con)titolare del trattamento o un altro responsabile del trattamento, oltre al titolare del trattamento o al responsabile del trattamento con cui l'interessato è in contatto diretto.

> **Example 32:** Un fornitore di social media collabora con terzi per il trattamento dei dati personali dei suoi utenti. Nella sua politica sulla privacy fornisce l'elenco di tali terzi senza includere un link a ciascuna delle rispettive politiche sulla privacy, ma si limita a invitare gli utenti a visitare i siti web dei terzi per ottenere informazioni su come questi trattano i dati e per esercitare i propri diritti.

114. Questo esempio di modello di ***punto morto*** mostra come l'accesso alle informazioni sul rispettivo trattamento sia reso più difficile per gli utenti. Data la probabilità che essi non ricevano tutte le informazioni pertinenti sul trattamento, si potrebbe ritenere che tale pratica violi i requisiti di cui all'articolo 12, paragrafo 1, GDPR, secondo i quali le informazioni devono essere facilmente accessibili. Se applicata alle informazioni fornite per ottenere il consenso, tale pratica può violare i requisiti del consenso informato di cui all'articolo 7, paragrafo 2, in combinato disposto con l'articolo 4, punto 11), GDPR, in quanto reperire le informazioni sarebbe troppo difficoltoso e pertanto gli interessati non sarebbero pienamente consapevoli delle conseguenze della propria scelta.

Obstructing — Allungare più del necessario (lista di controllo 4.4.2 dell'allegato I)

115. L'articolo 7, paragrafo 3, GDPR stabilisce che il consenso dovrebbe essere revocato con la stessa facilità con cui è accordato. Le linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679 approfondiscono questo aspetto, precisando che dovrebbe essere possibile esprimere e revocare il consenso tramite lo stesso mezzo. Ciò comporta l'utilizzo della stessa interfaccia, ma implica anche che i meccanismi per revocare il consenso dovrebbero essere facilmente accessibili, ad esempio attraverso un link o un'icona disponibili in qualsiasi momento durante l'utilizzo della piattaforma dei social media.

> **Example 33:** Un fornitore di social media non prevede una procedura diretta di revoca (*opt-out*) del consenso al trattamento per finalità di pubblicità mirata, anche se il consenso (*opt-in*) richiede un solo click.

116. Il tempo necessario o il numero di clic necessari per la revoca del consenso possono essere utilizzati per valutare se questa operazione sia effettivamente facile da realizzare. L'attuazione del modello di progettazione ingannevole consistente nell'***allungare più del necessario*** il percorso per la revoca del consenso da parte dell'utente, illustrato nell'esempio 33, è contraria a tali principi e viola pertanto l'articolo 7, paragrafo 3, GDPR.

Overloading – Privacy intricata (Allegato lista di controllo I 4.1.2)

117. Come sottolineato nelle linee guida 5/2020 sul consenso, agli interessati devono essere fornite informazioni in merito al fatto che il trattamento si basa sul consenso, affinché questi possano prendere decisioni informate[59]. In mancanza di tali informazioni, il consenso non può essere considerato valido. Le stesse Linee guida specificano inoltre i modi in cui le informazioni possono essere presentate, precisando che a tal fine possono essere utilizzate informazioni "a livelli". Tuttavia, come evidenziato nel caso d'uso n. 2a[60], quando forniscono informazioni riguardanti la richiesta del consenso con una modalità "a più livelli", i fornitori di social media devono sempre prestare attenzione a evitare il modello di progettazione ingannevole della ***privacy intricata***. Se alcune informazioni diventano troppo difficili da reperire in quanto gli interessati dovrebbero consultare più pagine o documenti, il consenso ottenuto fornendo tali informazioni non potrebbe essere considerato informato, in quanto non sarebbe conforme all'articolo 7 del GDPR in combinato disposto con l'articolo 4, punto 11), GDPR. Per analogia, ciò significherebbe che il consenso non è valido e che il fornitore di social media violerebbe l'articolo 6 GDPR.

> **Example 34:** Le informazioni per revocare il consenso sono disponibili attraverso un link cui si può accedere solo consultando tutte le sezioni del proprio account e le informazioni collegate agli annunci pubblicitari visualizzati sul *feed* dei social media.

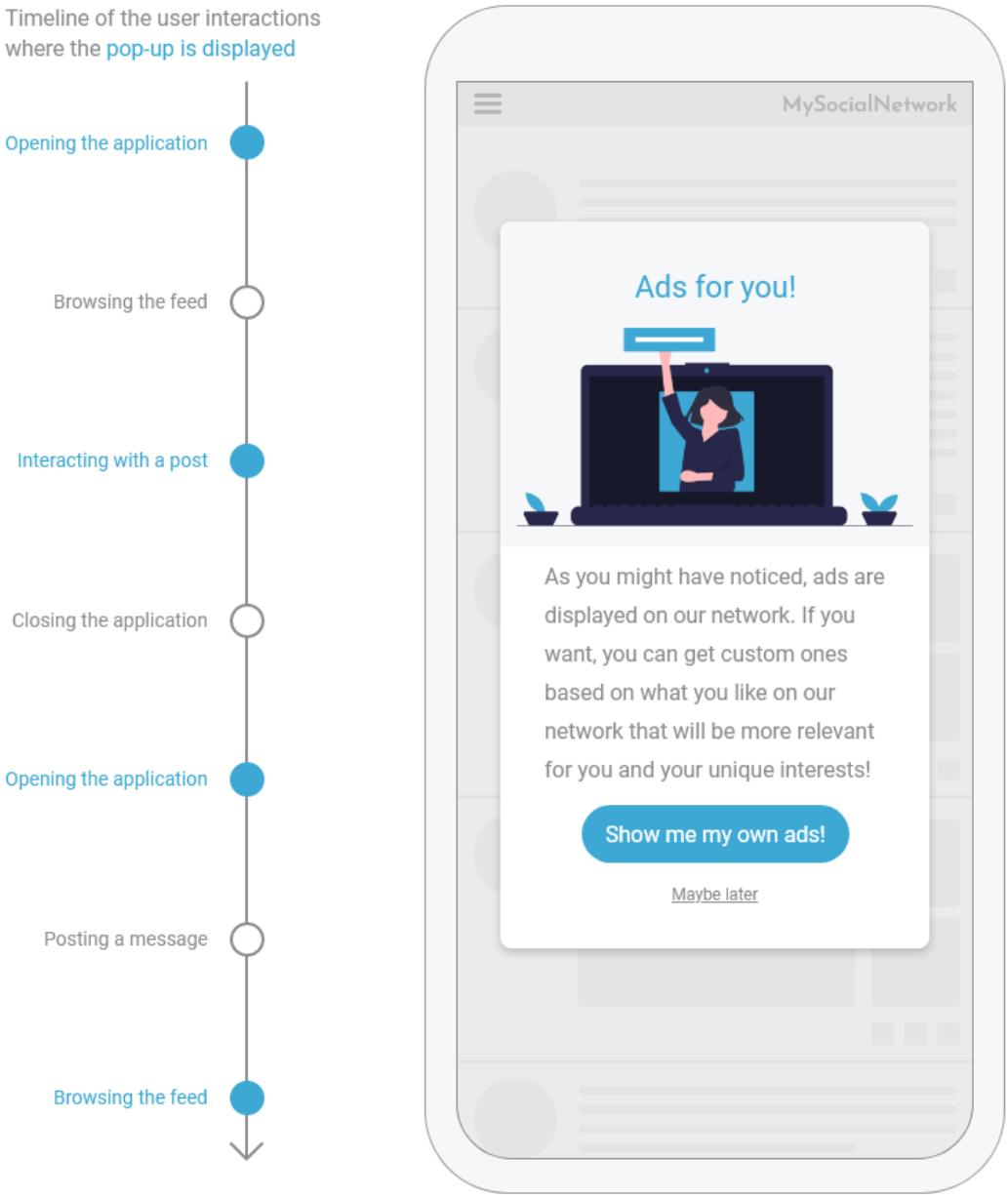
118. Come mostra lo scenario sopra descritto, il modello ingannevole della ***privacy intricata*** può costituire un problema anche dopo l'ottenimento del consenso, a causa del mancato rispetto della condizione di cui all'articolo 7, paragrafo 3, quarta frase, GDPR, che sancisce che il consenso è revocato con la stessa facilità con cui è accordato. La mancanza di conformità discende in particolare dal fatto che il processo di revoca del consenso prevede più passaggi rispetto all'azione positiva di espressione del consenso. Dato che le informazioni fornite non sono facilmente accessibili all'interessato, in quanto sono distribuite in punti diversi della pagina, è violato il principio di cui all'articolo 12, paragrafo 1, GDPR.

Overloading — Sollecitazione continua (lista di controllo 4.1.1 dell'allegato I)

119. La ***sollecitazione continua***, se utilizzata nei confronti di utenti che non hanno acconsentito al trattamento dei propri dati personali per una finalità specifica, crea un impedimento al normale utilizzo dei social media, in quanto gli utenti non possono negare il consenso e, per analogia, revocarlo senza subire pregiudizio. Ciò è in contrasto con la condizione di manifestazione di volontà libera del consenso di cui all'articolo 7, in combinato disposto con l'articolo 4, punto 11), GDPR, secondo cui per consenso si intende qualsiasi manifestazione di volontà libera dell'interessato con la quale lo stesso manifesta il proprio assenso a che i dati personali che lo riguardano siano oggetto di trattamento. Il considerando 42, quinta frase, GDPR afferma inoltre che il consenso non può essere considerato liberamente espresso se l'utente non è in grado di operare una scelta autenticamente libera. Tale considerazione è confermata anche nelle linee guida sul consenso dell'EDPB, in cui si spiega che il consenso non sarà valido se l'interessato non dispone di una scelta effettiva o se si sente obbligato ad acconsentire a causa di eventuali azioni di pressione o influenza inappropriata nei suoi confronti che gli impedisce di esercitare il suo libero arbitrio[61]. Dato che la ***sollecitazione continua*** può provocare tale tipo di pressione, ciò viola il principio del consenso liberamente espresso. Inoltre, essendo improbabile che, dopo averlo ottenuto, il fornitore di social media offra regolarmente agli utenti (ad esempio ogni volta

[59] Linee guida 5/2020 sul consenso, punti 62-64.
[60] Cfr. sopra, punti 79-81.
[61] Linee guida 5/2020 sul consenso, punti 13-14.

che accedono al loro account) la possibilità di revocare il consenso espresso, un simile modello di progettazione ingannevole può violare l'articolo 7, paragrafo 3, frase 4, GDPR, che sancisce che il consenso è revocato con la stessa facilità con cui è accordato ("effetto speculare").



Example 35: In questo esempio, quando crea il proprio account l'utente è invitato a indicare se acconsente al trattamento dei propri dati per finalità di pubblicità personalizzata. Nel caso in cui al momento dell'iscrizione non acconsenta a tale utilizzo dei propri dati, durante l'uso del social network l'utente vedrà comparire continuamente la casella sopra raffigurata, in cui si chiede all'utente se desidera ricevere annunci personalizzati. La casella interferisce con l'utilizzo del social network da parte dell'utente. Esasperato da tale ***sollecitazione continua***, questi potrebbe finire col prestare il consenso alla pubblicità personalizzata. Inoltre in questa

interfaccia è utilizzato anche il modello della ***poca visibilità***[62], in quanto l'azione per accettare gli annunci pubblicitari è molto più visibile dell'opzione per rifiutarli.

120. Inoltre il titolare del trattamento potrebbe violare il principio di correttezza ai sensi dell'articolo 5, paragrafo 1, lettera a), GDPR. Dato che, nell'esempio di cui sopra, al momento della creazione dell'account l'utente ha negato il consenso mediante un'azione inequivocabile al trattamento dei propri dati personali per la pubblicità mirata, la continua riproposizione della richiesta, che mette in discussione il rifiuto inequivocabile da questi espresso, è un elemento di onerosità. L'azione inequivocabile compiuta dall'utente durante il processo di registrazione è ora costantemente messa in discussione. Il conseguente peggioramento dell'esperienza dell'utente aumenta notevolmente la probabilità che questi finisca con l'accettare la pubblicità mirata pur di non vedersi rinnovare la richiesta ogni volta che accede al proprio account o che desidera utilizzare la piattaforma di social media. In questo caso, il fatto che l'utente non dia il proprio consenso incide direttamente sulla qualità del servizio offertogli e condiziona l'esecuzione del contratto.

c. Migliori prassi

Coerenza tra i diversi dispositivi: quando la piattaforma di social media è disponibile tramite dispositivi diversi (ad esempio computer, smartphone ecc.), le impostazioni e le informazioni relative alla protezione dei dati dovrebbero essere situate negli stessi spazi nelle diverse versioni e dovrebbero essere accessibili attraverso lo stesso percorso e gli stessi elementi di interfaccia (menu, icone ecc.).

Individuazione delle modifiche e confronto: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Formulazioni coerenti: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Fornitura di definizioni: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Uso di esempi: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Menu di navigazione "*sticky*" (fisso): per la definizione cfr. il caso d'uso n. 2a (pag. 28).

Inizio pagina: per la definizione cfr. il caso d'uso n. 2a (pag. 28).

Notifiche: per la definizione cfr. il caso d'uso n. 2c (pag. 32).

Spiegazione delle conseguenze: per la definizione cfr. il caso d'uso n. 2c (pag. 32).

Caso d'uso n. 3b: gestione delle impostazioni di protezione dei dati

a. Descrizione del contesto

121. Dopo aver completato il processo di iscrizione e durante l'intero ciclo di vita del loro account sui social media, gli utenti dovrebbero essere in grado di modificare le proprie impostazioni di protezione dei dati.

122. Tutti gli utenti, indipendentemente dal fatto che siano o meno già a conoscenza della protezione dei dati in generale e del GDPR in particolare, e che siano attenti ai dati personali che desiderano

[62]Cfr. il punto 49 o infra nella parte 4.3.2 dell'allegato.

condividere con altri e che desiderano che siano visualizzati da altri, hanno il diritto di essere informati in modo trasparente delle scelte a loro disposizione durante l'utilizzo dei social media.

123. Gli utenti condividono molti dati personali sulle piattaforme di social media. Sono spesso incoraggiati dalle piattaforme di social media a continuare a condividerne sempre di più in modo regolare. Anche se gli utenti potrebbero voler condividere momenti della loro vita, partecipare a un dibattito su una questione o ampliare le loro reti di contatti per motivi professionali o personali, è necessario dar loro gli strumenti per controllare chi può vedere quali parti dei loro dati personali. Un modo per evitare di moltiplicare il numero di passaggi necessari per modificare la propria impostazione consisterebbe nel progettare un pannello di controllo della privacy che consenta di centralizzare le impostazioni e facilitare il controllo dei dati da parte degli utenti.

b. Disposizioni normative pertinenti

124. Come indicato in precedenza[63], tra i principi fondamentali applicabili al trattamento dei dati personali, l'articolo 5, paragrafo 1, lettera a), GDPR stabilisce che i dati personali devono essere trattati in modo lecito, corretto e, aspetto di particole importanza in questo contesto, in modo trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza"). In base al principio di responsabilizzazione di cui all'articolo 5, paragrafo 2, GDPR, i titolari del trattamento sono tenuti a comprovare quali misure stanno adottando per rendere le proprie attività di trattamento non solo lecite e corrette, ma anche trasparenti. In questo caso d'uso sono pertinenti anche i principi di minimizzazione di cui all'articolo 5, paragrafo 1, lettera c), e di protezione dei dati fin dalla progettazione e per impostazione predefinita ai sensi dell'articolo 25 GDPR.

c. Modelli di progettazione ingannevoli

i. Modelli basati sui contenuti

125. Il primo problema che gli utenti incontrano in questo contesto riguarda la collocazione pratica delle impostazioni relative alla protezione dei dati. Gli utenti potrebbero leggere l'informativa sulla protezione dei dati e decidere quindi di apportare modifiche al trattamento dei loro dati personali. Potrebbero anche desiderare di farlo, senza aver letto l'informativa, nell'ambito del semplice utilizzo del social media, ad esempio quando si rendono conto che un'informazione pubblicata su una piattaforma di social media (ad esempio una foto sulla spiaggia con la propria famiglia) è condivisa con un gruppo con cui non desiderano condividerla (ad esempio i colleghi di lavoro). In ogni caso, il principio di trasparenza richiede che le opzioni di impostazione siano facilmente accessibili e siano disponibili in modo comprensibile. Tale obiettivo potrebbe essere conseguito raggruppando le impostazioni dei dati e della privacy in un'unica posizione utilizzando un URL intuitivo come [social-network.com]/impostazioni dei dati.

126. Esistono diversi modelli di progettazione legati a tale aspetto che rendono difficile per gli utenti trovare le impostazioni. I progettisti delle piattaforme di social media dovrebbero pertanto fare attenzione a evitare questi modelli di progettazione ingannevoli.

Overloading — Troppe opzioni (lista di controllo 4.1.3 dell'allegato I)

[63] Cfr. sopra, punti 1, 9, 10 e da 14 a 16.

127. Le impostazioni di protezione dei dati devono essere facilmente accessibili e seguire un ordine logico. Le impostazioni relative allo stesso aspetto della protezione dei dati dovrebbero preferibilmente trovarsi in un'unica posizione ben visibile. In caso contrario gli utenti si troveranno di fronte a troppe pagine da consultare e leggere, il che renderà eccessivamente impegnativo impostare le proprie preferenze in materia di protezione dei dati. Di fatto, di fronte a ***troppe opzioni*** tra cui scegliere, gli utenti potrebbero non essere in grado di compiere alcuna scelta o essere indotti a trascurare alcune impostazioni, finendo per rinunciare a impostare le proprie preferenze in materia di protezione dei dati oppure per farlo solo in parte. In questo caso sono violati i principi di trasparenza e correttezza. In particolare, questo modello può violare l'articolo 12, paragrafo 1, GDPR poiché rende difficile trovare un controllo specifico relativo alla protezione dei dati, dal momento che l'argomento è trattato su più pagine, oppure rende poco chiara la differenza tra le diverse opzioni fornite agli utenti.

> **Example 36:** È probabile che gli utenti non sappiano come agire quando il menu di una piattaforma di social media contiene più schede riguardanti la protezione dei dati, ad esempio "*protezione dei dati*", "*sicurezza*", "*contenuto*", "*privacy*", "*preferenze*".

128. In questo esempio i titoli delle schede non indicano chiaramente quali contenuti gli utenti possono aspettarsi nelle pagine associate o il fatto che tutte le schede riguardano la protezione dei dati, in particolare perché una delle schede è intitolata proprio "protezione dei dati". In tal modo si rischia di impedire agli utenti di apportare modifiche. Ad esempio, se desiderano limitare o ampliare il numero di persone che possono visualizzare le immagini che hanno caricato, i nomi delle schede potrebbero indurli a cliccare su "sicurezza", qualora ritengano che rendere i propri dati accessibili al pubblico comporti rischi per la sicurezza; su "contenuto", quando desiderano impostare la visibilità del proprio post; o su "privacy", in quanto questo concetto specifico si riferisce direttamente a ciò che si desidera condividere con gli altri. Di conseguenza questi titoli non sono sufficientemente chiari per quanto riguarda l'azione che gli utenti vorrebbero compiere. In particolare, i termini "protezione dei dati" e "privacy" sono spesso utilizzati come sinonimi e possono quindi ingenerare una certa confusione se presentati come titoli di sezioni diverse.

Left in the dark — Informazioni contrastanti (lista di controllo 4.6.2 dell'allegato I)

129. Come già descritto nell'esempio 12 e ulteriormente illustrato nell'esempio che segue, le ***informazioni contrastanti*** possono essere fornite agli utenti anche nel contesto delle impostazioni relative alla protezione dei dati.

> **Example 37:** L'utente X disattiva l'uso della propria geolocalizzazione per finalità pubblicitarie. Dopo aver cliccato sulla levetta che consente di farlo, gli appare il messaggio seguente: *"Abbiamo disattivato la tua geolocalizzazione, ma la tua posizione sarà ancora utilizzata"*.

Overloading — Privacy intricata (lista di controllo 4.1.2 dell'allegato I)

130. Quando gli utenti modificano un'impostazione relativa alla protezione dei dati, il principio di correttezza impone ai fornitori di social media di informare gli utenti anche in merito ad altre impostazioni simili. Se tali impostazioni sono distribuite in pagine diverse, non collegate alla piattaforma di social media, è probabile che agli utenti sfuggano uno o più mezzi per controllare un aspetto dei propri dati personali. Gli utenti si aspettano di trovare le impostazioni vicine tra loro.

Example 38: Gli argomenti collegati, come le impostazioni sulla condivisione dei dati da parte del fornitore di social media con terzi e viceversa, non sono messi a disposizione nello stesso spazio o in spazi vicini, ma si trovano invece in diverse schede del menu delle impostazioni.

131. Non esiste un approccio unico valido per tutti per quanto riguarda il numero medio di passaggi che gli utenti dei social media possono considerare tollerabili per cambiare un'impostazione. Allo stesso tempo, un numero elevato di passaggi può far desistere gli utenti dal portare a termine la modifica o può far sfuggire loro alcuni elementi, soprattutto se desiderano apportare più modifiche. Ostacolare in tal modo la volontà degli utenti viola i principi di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR. Inoltre la modifica delle impostazioni è strettamente connessa all'esercizio dei diritti dell'interessato[64]. La modifica di un'impostazione relativa ai dati, come la rettifica del nome o la cancellazione dell'anno di laurea, può essere considerata un esercizio del diritto di rettifica, oppure del diritto alla cancellazione, per questi dati specifici. Il numero di passaggi richiesti dovrebbe pertanto essere il minore possibile. Sebbene possa variare, un numero eccessivo di passaggi ostacola gli utenti e viola pertanto il principio di correttezza nonché l'articolo 12, paragrafi 1 e 2, GDPR.

Fickle — Discontinuità linguistica (lista di controllo 4.5.4 dell'allegato I)

132. Per quanto riguarda la trasparenza delle informazioni, i progettisti delle piattaforme di social media devono anche prestare attenzione a evitare i modelli di progettazione ingannevoli basati sui contenuti elencati nel caso d'uso n. 2a, come la ***discontinuità linguistica***. Se le pagine relative alle impostazioni (o parti di esse) non sono disponibili nella lingua scelta dall'utente per la piattaforma di social media, sarà più difficile per l'utente comprendere cosa può modificare e quindi impostare le proprie preferenze.

Fickle — Interfaccia incoerente (lista di controllo 4.5.3 dell'allegato I)

133. In questo contesto, un altro problema si verifica quando le piattaforme di social media presentano agli utenti scelte che facilitano la protezione dei dati, ma non li informano in modo chiaro. Ciò può accadere quando il modello di progettazione della piattaforma di social media si discosta improvvisamente da quello abituale. Questo tipo di ***interfaccia incoerente*** si verifica quando un'interfaccia non è coerente nei diversi contesti o rispetto alle aspettative degli utenti. Tali differenze possono far sì che gli utenti non trovino il controllo o le informazioni desiderati oppure che, per abitudine, interagiscano con un dato elemento dell'interfaccia, anche se tale interazione li porta a compiere una scelta non voluta in materia di protezione dei dati.

Example 39: In tutta la piattaforma di social media, nove opzioni di impostazione della protezione dei dati su dieci sono presentate nell'ordine seguente:

— opzione più restrittiva (ossia condivisione della minor quantità di dati con gli altri)

— opzione con limitazioni, ma meno restrittiva della prima

— opzione meno restrittiva (ossia condivisione della maggior quantità di dati con gli altri).

[64] Cfr. di seguito i casi d'uso nn. 4 e 5, ossia le sezioni 3.4 e 3.5 delle presenti linee guida.

Gli utenti della piattaforma sono abituati a visualizzare le impostazioni di protezione dei dati in questo ordine. Tuttavia tale ordine non è applicato all'ultima impostazione, in cui le scelte relative alla visibilità del compleanno dell'utente sono indicate nell'ordine seguente:

— mostra la data completa del mio compleanno: 15 gennaio 1929 (= opzione meno restrittiva)

— *mostra solo giorno e mese: 15 gennaio* (= opzione con limitazioni, ma non la più restrittiva)

— non mostrare agli altri il mio compleanno (= opzione più restrittiva).

134. Nell'esempio, le tre scelte dell'ultima impostazione sono presentate in un ordine diverso da quello fornito nelle impostazioni precedenti. Se in precedenza ha modificato le altre impostazioni, l'utente si sarà probabilmente abituato all'ordine "solito" presente nelle precedenti nove. Giunto all'ultima impostazione, sarà così abituato a tale ordine da scegliere istintivamente la prima opzione, presumendo che si tratti di quella più restrittiva. Organizzare le opzioni relative a una delle impostazioni di protezione dei dati in modo così diverso rispetto a quello in cui sono organizzate le altre opzioni della piattaforma di social media rende l'***interfaccia incoerente***, in quanto gioca con le abitudini e con le aspettative dell'utente. In tal modo si può ingenerare confusione o indurre l'utente a credere di avere compiuto la scelta desiderata, quando in realtà non è così.

ii. Modelli basati sull'interfaccia

135. Il secondo aspetto problematico da affrontare nel contesto delle impostazioni di protezione dei dati consiste nella possibilità che le impostazioni violino il principio della protezione dei dati fin dalla progettazione. L'articolo 25, paragrafo 1, GDPR impone ai titolari del trattamento di mettere in atto misure adeguate volte ad attuare i principi di protezione dei dati, quali la minimizzazione dei dati (articolo 5, paragrafo 1, lettera c), GDPR). Tali disposizioni non sono rispettate quando le impostazioni relative alla condivisione dei dati personali sono preimpostate su una delle opzioni più invasive invece che su quella meno invasiva.

Skipping — Comodità ingannevole (lista di controllo 4.2.1 dell'allegato I)

Example 40: Tra le opzioni di visibilità dei dati *"visibile a me", "ai miei amici più stretti" "a tutti i miei contatti"* e *"pubblico"*, è preimpostata l'opzione intermedia "a tutti i miei contatti". Ciò significa che tutti gli utenti collegati con l'utente possono vedere i suoi contributi, come pure tutte le informazioni inserite per iscriversi sulla piattaforma di social media, tra cui l'indirizzo e-mail o la data di nascita.

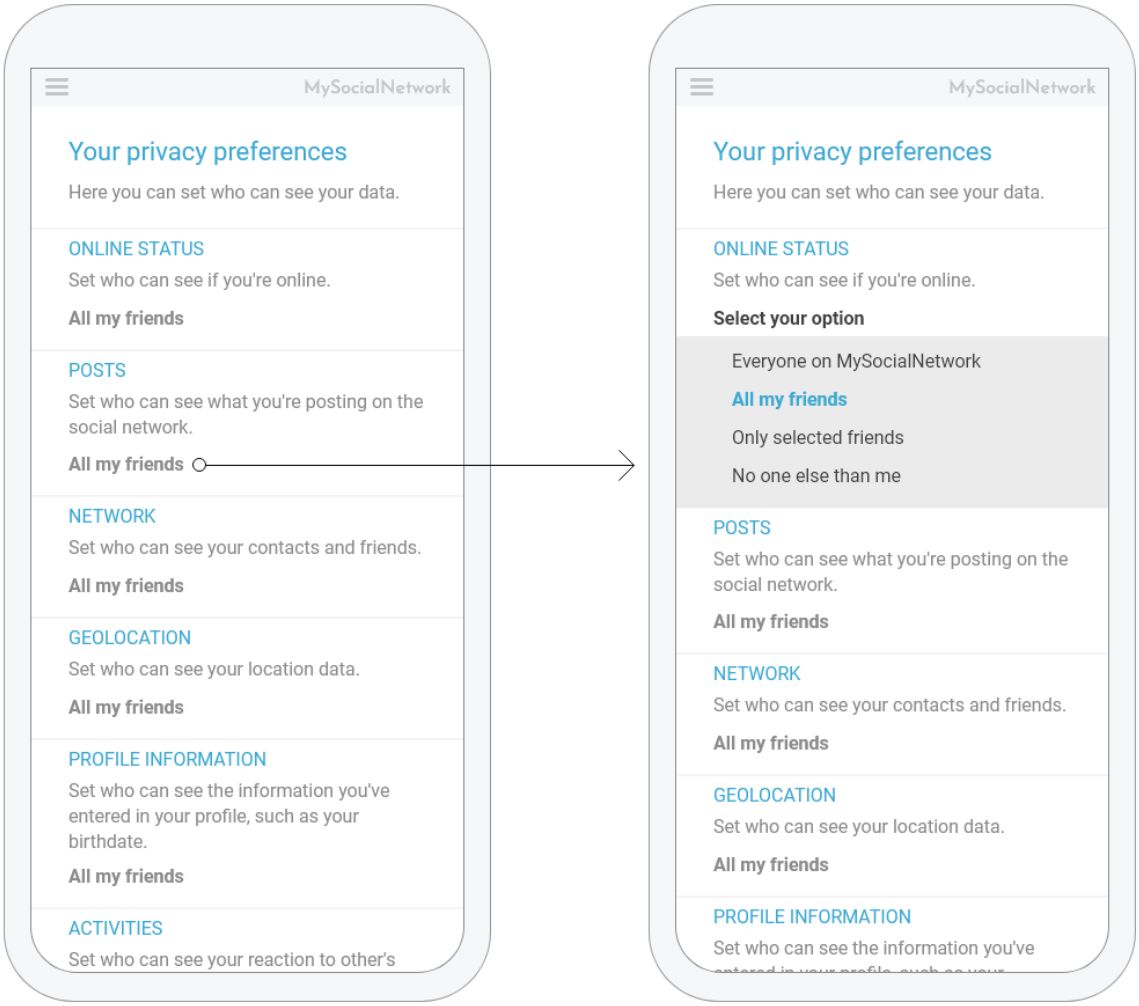
136. I fornitori di social media potrebbero sostenere che l'impostazione meno invasiva vanificherebbe l'obiettivo degli utenti di una determinata piattaforma di social media, ad esempio quello di essere contattati da persone sconosciute in modo da trovare nuove amicizie, nuovi partner o un nuovo lavoro. Sebbene ciò possa essere vero per alcune impostazioni specifiche, i fornitori di social media devono tenere presente che il fatto che gli utenti carichino determinati dati sulla rete non costituisce un consenso alla condivisione di tali dati con altri[65]. Qualora non si attengano alla protezione dei dati per impostazione predefinita, i fornitori di social media dovranno avere cura di informare adeguatamente gli utenti al riguardo. Pertanto gli utenti devono essere a conoscenza di quale sia l'impostazione

[65] Ad esempio la data di nascita, cfr. il precedente punto 58.

predefinita, della disponibilità di opzioni meno invasive e della sezione della piattaforma in cui recarsi per effettuare le modifiche. Nell'esempio in questione questo significa che, quando per i contributi che gli utenti pubblicano attivamente sulla piattaforma di social media è preimpostata l'opzione "*ai miei amici più stretti*", dovrebbe essere mostrata la sezione in cui modificare tale impostazione. Tuttavia la preimpostazione della visibilità per *"tutti i contatti dell'utente"* (o addirittura per il pubblico in generale) costituisce una ***comodità ingannevole***, in particolare se applicata ai dati che il fornitore di social media ha chiesto agli utenti per creare un account, come l'indirizzo di posta elettronica o la loro data di nascita. Come illustrato nel caso d'uso n. 1, punto 55, tale pratica viola l'articolo 25, paragrafo 2, GDPR.

Stirring — Poca visibilità (lista di controllo 4.3.2 dell'allegato I)

137. I modelli di progettazione ingannevoli della ***poca visibilità*** e della ***comodità ingannevole*** possono essere facilmente combinati per quanto riguarda la selezione delle opzioni relative alla protezione dei dati, come illustrato nell'esempio 9, relativo al processo di iscrizione, e nell'esempio che segue, in cui gli utenti desiderano modificare le proprie preferenze in materia di protezione dei dati nell'utilizzo del social media.



Example 41: In questo esempio, se desidera gestire la visibilità dei propri dati l'utente deve aprire la scheda *"preferenze sulla privacy"*. In tale scheda sono elencate le informazioni per le quali può impostare la propria preferenza. Tuttavia, a causa del modo in cui le informazioni sono visualizzate, le modalità di modifica delle impostazioni non risultano chiare. Gli utenti devono infatti cliccare sull'opzione di visibilità corrente per accedere a un menu a tendina dal quale possono selezionare l'opzione preferita.

138. Pur essendo disponibile nella scheda, la modifica delle preferenze è ***poco visibile***, in quanto gli utenti non visualizzano immediatamente il menu a tendina, ma devono immaginare che, cliccando sull'opzione corrente, qualcosa si aprirà. Non è infatti presente alcuna classica indicazione visiva (testo sottolineato, freccia discendente) della possibilità di interagire e aprire il menu a tendina. Quella descritta è una pratica scorretta nei confronti degli utenti e potrebbe contribuire alla generale inosservanza del principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR. Inoltre, se

le opzioni sono state preselezionate per impostazione predefinita, si potrebbe configurare anche il modello di progettazione ingannevole della ***comodità ingannevole***, descritto al punto 128.

Fickle — Decontestualizzazione (lista di controllo 4.5.2 dell'allegato I)

139. La ***decontestualizzazione*** avviene quando un'informazione o un controllo riguardante la protezione dei dati si trova su una pagina che è slegata dal contesto ed è pertanto improbabile che gli utenti riescano a trovare tale informazione o controllo in quanto non sarebbe intuitivo cercarli su quella pagina.

> **Example 42:** Le impostazioni relative alla protezione dei dati sono difficili da trovare nell'account utente, in quanto al primo livello non esiste una voce del menu con un nome o un titolo che porti in tale direzione. Gli utenti devono cercare in altri sottomenu, come ad esempio "*Sicurezza*".

140. In questo esempio gli utenti non sono guidati verso le impostazioni di protezione dei dati perché non vengono utilizzati termini chiari e significativi per indicare dove tali informazioni siano collocate nella piattaforma di social media. Infatti il termine "*sicurezza*" riguarda solo una piccola parte di ciò che ci si può aspettare dalle impostazioni relative alla protezione dei dati. Non è quindi intuitivo che gli utenti consultino questo menu per trovare tali impostazioni. Questa mancanza di trasparenza rende l'accesso alle informazioni più difficile di quanto dovrebbe e può essere considerata una violazione dell'articolo 12, paragrafo 1, GDPR, e potenzialmente dell'articolo 12, paragrafo 2, GDPR, se tali impostazioni riguardano l'esercizio di un diritto.

> **Example 43:** La modifica dell'impostazione è ostacolata dal fatto che, nella versione desktop della piattaforma di social media, il pulsante "*salva*" per registrare le modifiche non è visibile insieme a tutte le opzioni, ma soltanto in cima al sottomenu. È probabile che gli utenti non lo notino e, supponendo erroneamente che le loro impostazioni siano salvate in automatico, si spostino su un'altra pagina senza cliccare sul pulsante "*salva*". Questo problema non si verifica nelle applicazioni e nelle versioni mobili. Pertanto crea ulteriore confusione per gli utenti che passano dalla versione mobile/app alla versione desktop e può indurli a pensare di poter modificare le impostazioni solo nella versione mobile o nell'applicazione.

141. Una volta che gli utenti hanno trovato le impostazioni relative alla protezione dei dati e impostato le proprie scelte, non può essere loro impedito di agire in tal senso. Quando gli utenti apportano una modifica, il modo per salvarla deve essere ovvio, tanto se il salvataggio avviene contestualmente alla regolazione dell'impostazione, quanto se è necessario confermarlo cliccando su un elemento specifico dell'interfaccia, come il pulsante "Salva". Inoltre il principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR impone ai fornitori di social media di mantenere la coerenza in tutta la loro piattaforma, in particolare tra i diversi dispositivi. Ciò non si verifica quando l'interfaccia utilizza un modello di progettazione ingannevole come quello descritto negli esempi di cui sopra.

d. Migliori prassi

Directory della protezione dei dati: per facilitare l'orientamento attraverso le diverse sezioni del menu, fornire agli utenti una pagina facilmente accessibile dalla quale possano accedere a tutte le funzioni (ad esempio le impostazioni) e informazioni relative alla protezione dei dati. La pagina si può trovare nel menu principale di navigazione del fornitore di social media, nell'account utente, attraverso la politica sulla privacy ecc.

Raggruppamento di opzioni: riunire opzioni che hanno la stessa finalità di trattamento in modo che gli utenti possano modificarle più facilmente, pur lasciando agli utenti stessi la possibilità di apportare modifiche più granulari. Se le piattaforme di social media presentano raggruppamenti di opzioni, queste non dovrebbero contenere elementi imprevisti o non correlati (ad esempio elementi con finalità diverse). Se il trattamento è subordinato al consenso, i raggruppamenti di opzioni devono essere in linea con le linee guida dell'EDPB sul consenso, in particolare i punti da 42 a 44.

Scorciatoie: per la definizione cfr. il caso d'uso n. 1 (pag. 22) *(ad esempio, quando sono informati di un aspetto del trattamento, gli utenti sono invitati a impostare le loro preferenze riguardo ai dati sulla corrispondente pagina delle impostazioni/del pannello di controllo)*.

Significato intuitivo dell'URL: le pagine relative alle impostazioni o alle informazioni sulla protezione dei dati dovrebbero utilizzare un indirizzo web che ne rifletta chiaramente il contenuto. Ad esempio una pagina che centralizza il controllo della protezione dei dati potrebbe avere un URL del tipo [social-network.com]/impostazioni-dati.

Formulazioni coerenti: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Fornitura di definizioni: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Uso di esempi: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Menu di navigazione "*sticky*" (fisso): per la definizione cfr. il caso d'uso n. 2a (pag. 28).

Notifiche: per la definizione cfr. il caso d'uso n. 2c (pag. 32).

Spiegazione delle conseguenze: per la definizione cfr. il caso d'uso n. 2c (pag. 32).

Coerenza tra i diversi dispositivi: per la definizione cfr. il caso d'uso n. 3a (pag. 39).

3.4 Rimanere dal lato dei diritti sui social media: i diritti degli interessati

Caso d'uso n. 4: come fornire funzioni adeguate per l'esercizio dei diritti degli interessati

a. Descrizione del contesto

142. Utilizzare una piattaforma di social media significa sfruttare le sue funzioni secondo le finalità dichiarate dal fornitore di social media. Ciò significa anche che gli utenti devono poter esercitare i propri diritti in materia di protezione dei dati. Si tratta di elementi fondamentali della protezione dei dati e del controllo delle proprie informazioni, indipendentemente dal fatto che i dati siano forniti direttamente e consapevolmente dall'interessato, siano forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo, o siano dedotti dall'analisi di dati forniti dall'interessato[66]. Data la quantità di dati personali che circolano attraverso la piattaforma, gli utenti devono poter controllare i propri dati in modo chiaro e intuitivo avvalendosi dei diritti previsti dal GDPR. L'EDPB ha spiegato tali concetti in diverse linee guida[67]. L'esercizio dei diritti deve essere disponibile dall'inizio fino alla fine dell'utilizzo della piattaforma e, in alcuni casi, anche dopo che gli utenti hanno deciso di lasciare la piattaforma e il titolare del trattamento non ha ancora cancellato i loro dati. Anche coloro

[66] Cfr. Gruppo di lavoro articolo 29 per la protezione dei dati, Linee guida sul diritto alla portabilità dei dati, WP242 rev.01,, pag. 10, https://ec.europa.eu/newsroom/article29/items/611233/en.

[67] Linee guida sul diritto alla portabilità dei dati e EDPB, *Linee guida 5/2019 sui criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca ai sensi del GDPR (parte 1)* — versione adottata previa consultazione pubblica, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_it.

che non sono utenti della piattaforma devono essere autorizzati a esercitare i diritti degli interessati relativi al trattamento dei loro dati. Naturalmente, a seconda della base giuridica del trattamento dei dati, in alcuni casi non tutti i diritti dell'interessato sono disponibili. Il fornitore di social media dovrebbe pertanto anche spiegare chiaramente perché determinati diritti non sono applicabili e perché alcuni di essi possono essere limitati. Come indicato anche nei capitoli precedenti, l'esercizio dei diritti deve essere reso attivabile. L'automazione e altre funzionalità delle piattaforme di social media dovrebbero essere utilizzate per facilitare l'esercizio dei diritti.

b. Disposizioni normative pertinenti

143. Il GDPR descrive sette diversi diritti che gli interessati possono esercitare a determinate condizioni (ad esempio la base giuridica del trattamento ecc.). L'articolo 15 del GDPR consente agli interessati di sapere se sia o meno in corso un trattamento di dati che li riguardano e di ottenerne l'accesso, ossia di ottenere ulteriori informazioni su tale trattamento, nonché di ricevere una copia di tali dati. L'articolo 16 GDPR illustra il diritto di rettifica che consente agli interessati di aggiornare i dati personali trattati dal titolare del trattamento. Il diritto alla cancellazione di cui all'articolo 17 GDPR consente agli interessati di ottenere la cancellazione dei dati personali che li riguardano. Il diritto di limitazione di trattamento di cui all'articolo 18 GDPR offre agli interessati la possibilità di interrompere temporaneamente il trattamento dei loro dati personali. L'articolo 20 GDPR introduce il diritto alla portabilità dei dati che consente agli interessati di ricevere i propri dati personali e di trasmetterli a un altro titolare del trattamento[68]. Gli interessati hanno inoltre il diritto di opporsi al trattamento dei loro dati personali a norma dell'articolo 21 GDPR. Infine l'articolo 22 GDPR conferisce agli interessati il diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato[69].

144. L'EDPB sottolinea che non tutti i diritti citati si applicheranno a tutte le piattaforme di social media, ma la loro applicazione dipenderà dalla base giuridica della piattaforma, dalle finalità del trattamento dei dati personali da parte di quest'ultima e dai tipi di servizi da essa forniti. Le differenze dovrebbero essere spiegate dal titolare del trattamento conformemente all'articolo 12 GDPR. Ciò significa che le informazioni sui diritti applicabili dovrebbero essere concise e chiare per gli utenti, indicando anche il motivo per cui determinati diritti non trovano applicazione. Una spiegazione di tal genere potrebbe limitare la quantità di comunicazioni con gli utenti quando cercano di esercitare taluni diritti. L'esercizio di un diritto dovrebbe essere facile e accessibile a norma dell'articolo 12, paragrafo 2, e la risposta a eventuali richieste dovrebbe essere fornita senza ingiustificato ritardo, come previsto dall'articolo 12, paragrafo 3, GDPR. Analogamente, la piattaforma di social media dovrebbe spiegare perché determinate richieste non possono essere soddisfatte e informare in merito alla possibilità di proporre reclamo a un'autorità di controllo designata, come previsto dall'articolo 12, paragrafo 4, GDPR. Pertanto i modelli di progettazione ingannevoli descritti in appresso potrebbero non essere applicabili a tutti i diritti sopra menzionati. Il diritto alla cancellazione è esaminato in dettaglio nel prossimo capitolo.

c. Modelli di progettazione ingannevoli

i. Modelli basati sui contenuti

[68] Tale diritto è ulteriormente approfondito nelle linee guida sul diritto alla portabilità dei dati.

[69] Cfr. anche Gruppo di lavoro articolo 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*, wp251rev.01, pag. 19 e seguenti, https://ec.europa.eu/newsroom/article29/items/612053/en.

Obstructing — Punto morto (allegato lista di controllo I 4.4.1)

145. Il modello di progettazione ingannevole del ***punto morto*** può incidere direttamente sulla facilità di accesso all'esercizio dei diritti. Quando i link che reindirizzano ai mezzi per esercitare un diritto non sono funzionanti o mancano spiegazioni chiare su come esercitare un diritto, gli utenti non saranno in grado di esercitarlo correttamente, il che viola l'articolo 12, paragrafo 2, GDPR.

> **Example 44:** L'utente clicca su "*esercita il tuo diritto di accesso*" nell'informativa sulla privacy, ma viene invece reindirizzato al proprio profilo, nel quale non è presente alcuna funzione relativa all'esercizio del diritto.

146. L'esempio summenzionato di modello di progettazione ingannevole evidenzia la necessità di fornire agli utenti un modo chiaro e intuitivo per esercitare i loro diritti conformemente all'articolo 12, paragrafi 1 e 2 GDPR, in quanto altrimenti potrebbero non essere in grado di esercitarli. Non è sufficiente confermare agli utenti l'esistenza dei diritti degli interessati, come previsto dall'articolo 12, paragrafo 1, GDPR (comprese le modalità di comunicazione) e in particolare dall'articolo 13, paragrafo 2, lettera b), e dall'articolo 14, paragrafo 2, lettera c), GDPR. Gli utenti devono anche essere in grado di esercitarli con facilità, preferibilmente attraverso uno strumento integrato nell'interfaccia della piattaforma, ad esempio un modulo dedicato. Ciò renderebbe anche più positiva l'esperienza dell'utente sulla piattaforma, visto che il fornitore si è adoperato per venire incontro alle aspettative degli utenti in merito al trattamento lecito dei dati personali e al controllo sui loro dati combinando l'esercizio dei diritti con altre funzionalità del servizio. Quando il servizio di piattaforma di social media consente una comunicazione bidirezionale tra gli utenti, così come tra il titolare del trattamento e gli utenti, non vi è motivo per cui il titolare del trattamento debba limitare il proprio canale di comunicazione per l'agevolazione delle richieste dell'interessato a un mezzo di comunicazione distinto, come la posta elettronica. Al tempo stesso gli interessati non dovrebbero essere costretti a recarsi sulla piattaforma per comunicare con il titolare del trattamento[70]. Inoltre, i titolari del trattamento non possono limitare tale diritto dell'interessato al diritto di copia, ma devono invece assicurarsi di fornire anche le informazioni di cui all'articolo 15, paragrafo 1, GDPR agli utenti che chiedono l'accesso ai propri dati[71].

Fickle — Discontinuità linguistica (lista di controllo 4.5.4 dell'allegato I)

> **Example 45:** Cliccando su un link relativo all'esercizio dei diritti degli interessati, le seguenti informazioni, al contrario del servizio, non sono fornite nella lingua o nelle lingue ufficiali del paese dell'utente. L'utente è invece reindirizzato a una pagina in inglese.

147. Tenendo presente il principio di trasparenza di cui all'articolo 5, paragrafo 1, lettera a), e all'articolo 12, paragrafo 1, GDPR, l'utente deve ricevere tutte le informazioni sui propri diritti in modo chiaro, semplice e comprensibile. Tale principio deve riguardare anche l'ubicazione dell'utente e la lingua utilizzata nel paese o nella giurisdizione in cui il servizio è offerto. Il fatto che l'utente confermi la propria capacità di usare una lingua straniera non esonera in alcun modo il titolare del trattamento dai propri obblighi. Lo stesso vale quando il fatto che l'utente comprenda altre lingue si può dedurre dalle sue attività. Le informazioni dovrebbero essere pertinenti e utili agli utenti che esercitano i loro diritti.

[70]Cfr. EDPB, *Linee guida 1/2022 sui diritti degli interessati — diritto di accesso*, punto 136, versione 1.0, https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf.
[71] Cfr. EDPB, Linee guida 1/2022, punti 131, 142 e 145.

Left in the dark — Formulazioni o informazioni ambigue (lista di controllo 4.6.3 dell'allegato I)

148. Per quanto riguarda i diritti degli interessati, gli utenti possono anche trovarsi di fronte al modello di progettazione ingannevole della ***formulazione o delle informazioni ambigue***, come illustrato nell'esempio che segue.

> **Example 46:** Nella piattaforma di social media non si afferma esplicitamente che gli utenti nell'UE hanno il diritto di proporre reclamo a un'autorità di controllo, ma si accenna solo al fatto che in alcuni paesi (non si specifica quali) vi sono autorità di protezione dei dati con cui il fornitore di social media collabora in merito ai reclami.

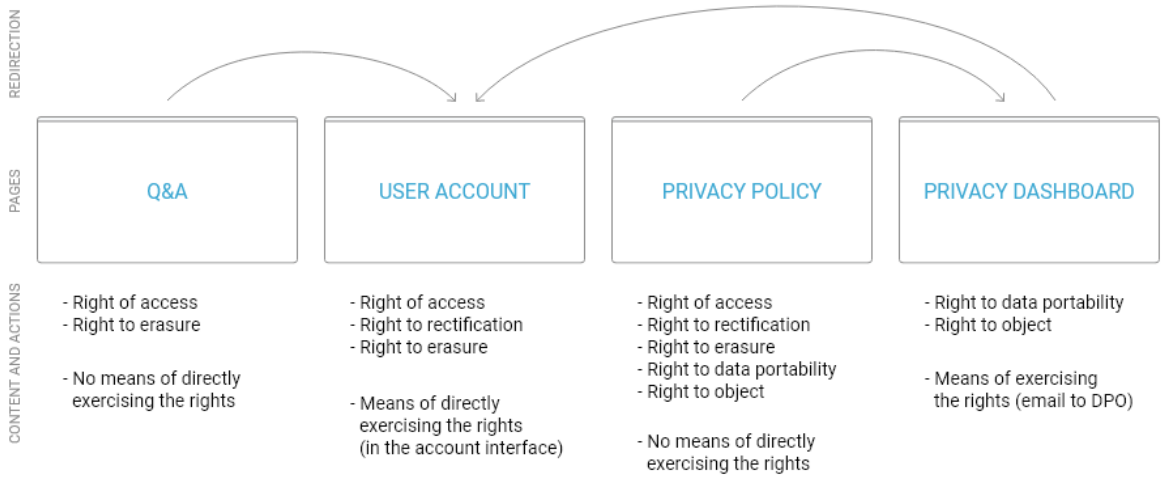
149. Nell'informare gli interessati in merito ai loro diritti, i fornitori di social media devono inoltre prestare attenzione a evitare il modello di progettazione ingannevole delle ***formulazioni o informazioni ambigue***. Fornire informazioni agli utenti in modo tale da renderli incerti su come i loro dati saranno trattati o su come avere un certo controllo su di essi e, di conseguenza, su come esercitare i propri diritti viola il principio di trasparenza. Inoltre una formulazione vaga non è un linguaggio conciso ai sensi dell'articolo 12, paragrafo 1, GDPR e può rendere incomplete le informazioni fornite all'interessato, per cui potrebbe essere considerata una violazione dell'articolo 13 GDPR. Dall'esempio sopra menzionato emerge anche una violazione dell'articolo 13, paragrafo 2, lettera d), GDPR, che impone ai titolari del trattamento di fornire agli interessati informazioni sul loro diritto di proporre reclamo a un'autorità di controllo. Per analogia, ciò è anche incompatibile con l'articolo 12, paragrafo 2, GDPR, in quanto il fornitore di social media non agevola l'esercizio del diritto di proporre reclamo.

ii. Modelli basati sull'interfaccia

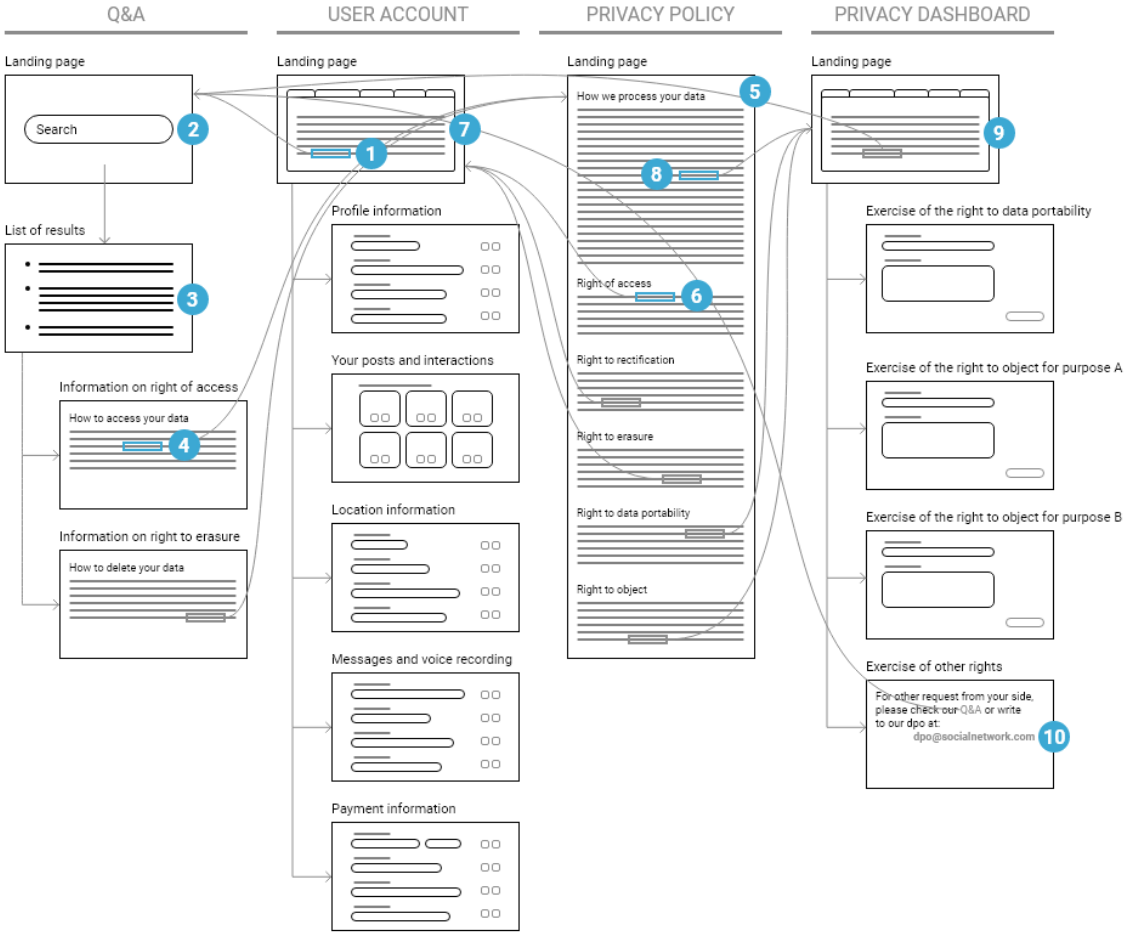
Overloading — Privacy intricata (lista di controllo 4.1.2 dell'allegato I)

150. Come descritto in precedenza nel caso d'uso n. 3b, il numero di passaggi necessari per ricevere le pertinenti informazioni sulla protezione dei dati non deve essere eccessivo, né può esserlo il numero di passaggi necessari per consultare i diritti dell'interessato[72]. Pertanto gli utenti dovrebbero sempre essere in grado di raggiungere rapidamente la sezione relativa all'esercizio dei diritti, indipendentemente dal punto in cui si trovano o da quello in cui la piattaforma di social media ha collocato tale funzionalità. I fornitori di social media dovrebbero pertanto riflettere attentamente sulle diverse situazioni in cui gli utenti potrebbero voler esercitare i propri diritti e progettare di conseguenza l'accesso alle pagine in cui possono farlo. Ciò significa che su una piattaforma di social media possono essere creati e messi a disposizione diversi percorsi per arrivare ai vari diritti dell'interessato. Ogni percorso dovrebbe però facilitare l'accesso all'esercizio dei diritti e non dovrebbe interferire con un altro percorso. In caso contrario, sarebbe considerato un modello di progettazione ingannevole di ***privacy intricata***, come illustrato negli esempi 47 e 48, in contrasto con le disposizioni dell'articolo 12, paragrafo 2, GDPR.

[72] Cfr. sopra, punto 123.



Example 47: In questo caso le informazioni relative ai diritti in materia di protezione dei dati sono esposte in almeno quattro pagine. Pur fornendo informazioni su tutti i diritti, la politica sulla privacy non rinvia alle pagine pertinenti a ciascuno di essi. Al contrario, visitando il proprio account, gli utenti non troveranno informazioni relative ad alcuni dei diritti che possono esercitare. A causa di tale ***privacy intricata*** gli utenti sono costretti ad aprire più pagine per trovare quella relativa all'esercizio di ciascun diritto e, a seconda della navigazione, potrebbero non venire a conoscenza di tutti i diritti di cui godono.



Example 48: In questo esempio l'utente desidera aggiornare alcuni dei propri dati personali, ma non trova un modo per farlo nel proprio account. Cliccando su un link (1) viene reindirizzato alla pagina "Domande e risposte", in cui inserisce la propria domanda (2). Appaiono diversi risultati (3), alcuni relativi ai diritti di accesso e di cancellazione. Dopo aver controllato tutti i risultati, clicca sul link disponibile nella pagina "Come accedere ai tuoi dati" (4). La pagina lo indirizza alla politica sulla privacy (5), dove trova informazioni su ulteriori diritti, consultate le quali clicca sul link associato all'esercizio del diritto di rettifica (6), che lo reindirizza all'account utente (7). Non soddisfatto, torna alla politica sulla privacy e clicca sul link generico "Invia una richiesta" (8). Da qui accede al suo pannello di controllo della privacy (9). Dato che nessuna delle opzioni disponibili sembra rispondere alle sue esigenze, l'utente apre la pagina "Esercizio di altri diritti" (10), in cui trova finalmente un indirizzo di contatto.

151. Entrambi gli esempi illustrano percorsi particolarmente lunghi ed estenuanti per l'esercizio dei propri diritti da parte dell'utente. Quando i mezzi per esercitare i vari diritti non figurano in un unico spazio, ma è disponibile una pagina che elenca tutti i diritti dell'interessato, tale pagina dovrebbe reindirizzare a ciascuno dei diversi spazi e non soltanto a uno o ad alcuni di essi, come accade nell'esempio 47. L'altro esempio illustra un percorso in cui l'utente non trova il mezzo per esercitare facilmente il diritto desiderato, nella fattispecie il diritto di rettifica, in quanto lo spazio abitualmente riservato a tale esercizio, vale a dire l'account utente, non gli fornisce il mezzo per farlo. L'utente cerca un altro modo

per esercitare tale diritto, ma non riesce a trovarne uno specifico e deve ricorrere a un mezzo generico fornito nel pannello di controllo della privacy.

152. Laddove siano stati progettati più percorsi per l'esercizio di un diritto, gli utenti dovrebbero sempre poter trovare agevolmente una panoramica dei diritti degli interessati. Le politiche sulla privacy dovrebbero essere chiare e potrebbero fungere da punto di accesso alle pagine in cui gli utenti possono esercitare i loro diritti. Tali documenti dovrebbero indicare tutti i diritti applicabili. Se uno di tali diritti non dovesse essere disponibile a causa di limitazioni di natura legale o tecnica, se ne dovrebbe fornire la spiegazione affinché gli utenti siano adeguatamente informati. La comprensione delle limitazioni dei trattamenti, dovute alla loro base o alle garanzie adottate dai titolari del trattamento, non è utile soltanto per gli utenti. Essa limita anche i casi in cui un fornitore di social media deve motivare l'impossibilità di soddisfare una richiesta relativa all'esercizio dei diritti dell'interessato presentata da un utente.

Stirring — Poca visibilità (lista di controllo 4.3.2 dell'allegato I)

153. La possibilità degli utenti di raggiungere la pagina attraverso cui esercitare i propri diritti può essere compromessa anche rendendo praticamente invisibili le informazioni o i link correlati, utilizzando cioè il modello di progettazione ingannevole della ***poca visibilità***.

> **Example 49:** Nella politica sulla privacy, il paragrafo in corrispondenza del sottotitolo "diritto di accesso" spiega che gli utenti hanno il diritto di ottenere informazioni ai sensi dell'articolo 15, paragrafo 1, GDPR. Tuttavia il paragrafo si limita a indicare la possibilità degli utenti di ricevere una copia dei loro dati personali e non contiene alcun link diretto visibile per l'esercizio della componente "copia" del diritto di accesso ai sensi dell'articolo 15, paragrafo 3, GDPR. Le prime due parole della frase "Puoi ottenere una copia dei tuoi dati personali" sono invece leggermente sottolineate. Quando posiziona il puntatore del mouse su queste parole, l'utente visualizza un piccolo riquadro con un link alle impostazioni.

154. Oltre a quanto indicato nella sezione precedente, qualsiasi mezzo creato dal titolare del trattamento per l'esercizio dei diritti dovrebbe essere facilmente accessibile. Questa regola non può essere sottovalutata. Un'azione da parte del titolare del trattamento come quella sopra descritta non può che essere considerata un tentativo di impedire l'esercizio dei diritti da parte degli utenti, il che viola l'articolo 12, paragrafo 2, GDPR. Indipendentemente dalle loro ragioni, i titolari del trattamento non dovrebbero ostacolare tale richiesta. A un esame più approfondito da parte di un'autorità di controllo in un caso specifico, ciò potrebbe configurare una violazione del GDPR e determinare l'irrogazione di sanzioni nei confronti del titolare del trattamento.

Fickle — Interfaccia incoerente (lista di controllo 4.5.3 dell'allegato I)

> **Example 50:** La piattaforma di social media offre diverse versioni (desktop, app, browser mobile). In ciascuna versione le impostazioni (che portano all'accesso/all'opposizione ecc.) sono visualizzate con un simbolo diverso, generando confusione negli utenti che passano da una versione all'altra.

155. Di fronte a interfacce dei diversi dispositivi che trasmettono le stesse informazioni mediante una varietà di segnalatori visivi, è probabile che gli utenti impieghino più tempo o abbiano difficoltà a trovare i comandi che conoscono nel passaggio da un dispositivo all'altro. Nell'esempio precedente, ciò è dovuto all'uso di simboli o icone diversi per indirizzare gli utenti verso le impostazioni. Creare una

simile confusione negli utenti potrebbe essere considerato in contrasto con l'agevolazione dell'esercizio dei diritti dell'interessato di cui all'articolo 12, paragrafo 2, GDPR.

Obstructing– Allungare più del necessario (lista di controllo 4.4.2 dell'allegato I)

156. Infine qualsiasi tentativo di ***allungare più del necessario*** i tempi per l'esercizio di un diritto può essere considerato contrario al GDPR.

> **Example 51:** Quando l'utente sceglie di cancellare il nome e il luogo della sua scuola superiore o il riferimento a un evento cui ha partecipato e che ha condiviso, si apre una seconda finestra in cui si chiede di confermare tale scelta ("*Vuoi davvero farlo*? *Per quale motivo? ")*.

157. Analogamente alla quantità dei livelli di una politica sulla privacy (caso d'uso n. 2a) e al numero di passaggi per raggiungere o modificare un'impostazione (caso d'uso n. 3b), anche la quantità di passaggi o di clic che gli utenti devono effettuare per esercitare un diritto non dovrebbe essere eccessiva. Tale aspetto dipende ovviamente dalla complessità delle operazioni condotte dal titolare del trattamento, tenendo conto del contesto specifico. Sarebbe tuttavia irragionevole imporre all'utente di compiere un numero elevato di azioni non necessarie per poter portare a termine l'esercizio di un proprio diritto. In particolare non si dovrebbe scoraggiare l'utente con ulteriori domande, chiedendogli ad esempio se intende davvero esercitare tale diritto o quali sono i motivi di tale richiesta. Nella maggior parte dei casi l'utente dovrebbe essere in grado di esercitare semplicemente il proprio diritto, senza che la sua motivazione sia messa in discussione. Simili pratiche, illustrate nell'esempio di cui sopra, possono essere considerate in contrasto con l'articolo 12, paragrafo 2, GDPR, in quanto il titolare del trattamento ostacola l'esercizio dei diritti prevedendo passaggi non necessari. Naturalmente ciò non significa che il titolare del trattamento non possa ricevere un riscontro ponendo in seguito ulteriori domande al fine di migliorare il servizio. Rivolgendo tali domande in un secondo momento, la scelta di rispondere dipenderebbe unicamente dalla volontà degli utenti e non sarebbe confusa con un presupposto per l'esercizio di un diritto.

d. Migliori prassi

Modulo per l'esercizio dei diritti: per agevolare gli utenti nell'esercizio dei propri diritti ai sensi del GDPR, fornire un apposito modulo che li aiuti a comprendere i loro diritti e li guidi nella presentazione di questo tipo di richieste.

Scorciatoie: per la definizione cfr. il caso d'uso n. 1 (pag. 22) (*ad esempio, fornire un link alla cancellazione dell'account nell'account utente*).

Formulazioni coerenti: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Fornitura di definizioni: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Uso di esempi: per la definizione cfr. il caso d'uso n. 1 (pag. 22).

Menu di navigazione "*sticky*" (fisso): per la definizione cfr. il caso d'uso n. 2a (pag. 28).

Spiegazione delle conseguenze: per la definizione cfr. il caso d'uso n. 2c (pag. 32).

Coerenza tra i diversi dispositivi: per la definizione cfr. il caso d'uso n. 3a (pag. 39).

Directory della protezione dei dati: per la definizione cfr. il caso d'uso n. 3b (pag. 45).

Relazioni sui controlli della protezione dei dati: per la definizione cfr. il caso d'uso n. 3b (pag. 45).

3.5 Addio e arrivederci: abbandonare un account sui social media

Caso d'uso n. 5: sospensione dell'account/cancellazione di tutti i dati personali

a. Descrizione del contesto e disposizioni giuridiche pertinenti

158. Per fine del ciclo di vita di un account si intende la situazione in cui l'utente decide di abbandonare il social network. Generalmente in tale situazione l'utente decide di lasciare la piattaforma dei social media in maniera definitiva. Tuttavia spesso esiste anche la possibilità di disattivare solo temporaneamente l'account e di sospendere il servizio. Le due decisioni hanno implicazioni giuridiche diverse che sono descritte in appresso.

i. Cancellazione permanente dell'account

159. La decisione di abbandonare definitivamente la piattaforma di social media è accompagnata dal diritto alla cancellazione di cui all'articolo 17, paragrafo 1, lettera a), GDPR. In questo contesto, il termine "eliminazione" è utilizzato con maggiore frequenza rispetto a "cancellazione".

160. Il termine "cancellazione" non è giuridicamente definito all'articolo 17 GDPR ed è menzionato solo come forma di trattamento nell'articolo 4, punto 2), GDPR. La cancellazione può essere generalmente intesa come un'impossibilità (fattuale) di visualizzare le informazioni su un interessato precedentemente contenute nei dati da cancellare. Dopo la cancellazione, nessuno deve avere più la possibilità di visualizzare le informazioni in questione senza uno sforzo sproporzionato.

161. L'anonimizzazione è un altro modo per eliminare definitivamente il rapporto con una persona. In altri termini, l'uso di tecniche di anonimizzazione mira a garantire che l'interessato non possa più essere identificato. L'anonimizzazione comporta anche la cessazione dell'applicabilità dei principi del diritto in materia di protezione dei dati, come il principio della limitazione delle finalità (cfr. considerando 26, quarta e quinta frase).

162. A norma dell'articolo 12, paragrafo 2, GDPR, il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. In base a tale obbligo non possono essere creati ostacoli sostanziali o formali all'esercizio dei diritti dell'interessato. Pertanto, se l'esercizio del diritto di cancellazione è reso più difficile senza un motivo concreto, ciò costituisce una violazione del GDPR. Sebbene i fornitori di social media abbiano un valido motivo per spiegare obiettivamente le conseguenze, ad esempio la cancellazione di tutti i dati personali, e per chiedere agli interessati di confermare tale scelta[73], anche in questo caso d'uso devono essere evitati ostacoli inutili. Ne consegue, ad esempio, che qualsiasi periodo di tolleranza tra la richiesta di cancellazione dell'account di un utente e l'effettiva cancellazione di tale account deve essere proporzionato. Pertanto la durata di tale periodo non può essere eccessiva, tenuto conto sia delle necessarie motivazioni tecniche alla base dei ritardi rispetto a una cancellazione immediata, sia di un breve lasso di tempo in cui gli utenti possano riflettere sulla cancellazione del loro account una volta avviata la relativa procedura. Se, da un lato, occorre rispettare la libera volontà dell'utente di cambiare idea, dall'altro i fornitori di social media non possono tentare di indurre l'utente a cambiare idea invitandolo a tornare sui suoi passi, il che equivarrebbe anche a ostacolare l'esercizio del diritto di cancellazione da parte dell'utente stesso. In alcuni casi, il processo di cancellazione potrebbe subire interruzioni durante il periodo di tolleranza, ad esempio quando l'utente effettua nuovamente l'accesso. Se la cancellazione non può essere completata, l'utente deve essere informato e ricevere indicazioni su come completare la stessa.

163. La decisione di abbandonare la piattaforma di social media comporta le conseguenze della cancellazione stabilite all'articolo 17, paragrafo 1, GDPR. Se un interessato chiede la cancellazione del

[73] Contrariamente agli altri diritti dell'interessato, cfr. il precedente punto 154.

proprio account, il titolare del trattamento di una piattaforma di social media deve cancellare i dati. Tuttavia alcuni dati possono rimanere sulla piattaforma di social media per un certo periodo di tempo se è applicabile l'articolo 17, paragrafo 3, GDPR. Le eccezioni elencate all'articolo 17, paragrafo 3, GDPR devono essere interpretate in senso restrittivo e si applicano solo nei casi esplicitamente menzionati in tale parte della disposizione. Qualsiasi eccezione invocata da un titolare del trattamento a norma dell'articolo 17, paragrafo 3, GDPR e la corrispondente conservazione dei dati devono essere da questi giustificate, ad esempio sulla base di un obbligo previsto dal diritto nazionale che imponga al titolare del trattamento di conservare le informazioni relative all'interessato per motivi imperativi di interesse pubblico, per l'esercizio del diritto fondamentale alla libertà di espressione e di informazione o per motivi fiscali. Va da sé che i dati rimanenti dovrebbero essere conservati solo internamente dal fornitore di social media e non dovrebbero essere pubblicamente visibili agli altri utenti. Tuttavia una deroga ai sensi dell'articolo 17, paragrafo 3, GDPR non consente in alcun modo al fornitore di social media, dopo la richiesta di cancellazione, di mantenere attivo l'account interessato più a lungo di quanto desiderato dall'utente.

164. Indipendentemente dalla richiesta di cancellazione dell'account, se l'utente revoca il proprio consenso a norma dell'articolo 7, paragrafo 3, GDPR, i dati forniti sulla base del consenso a norma dell'articolo 6, paragrafo 1, lettera a), GDPR non possono più essere sottoposti a trattamento. In questo caso, in determinate circostanze, il fornitore di social media potrebbe comunque condurre altre operazioni di trattamento fondate su altre basi giuridiche ai sensi dell'articolo 6, paragrafo 1, GDPR.

165. Tuttavia se l'utente chiede la cancellazione del proprio account, non dovrebbe aver luogo alcun ulteriore trattamento, indipendentemente dalla base giuridica sottostante, a meno che non si applichi una delle eccezioni elencate in modo esaustivo all'articolo 17, paragrafo 3, GDPR. In tale contesto è importante tenere presente che la conservazione è limitata al periodo di conservazione minimo di cui sopra.

166. Ai sensi dell'articolo 25, paragrafo 1, GDPR, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per attuare i principi di protezione dei dati. Secondo le *Linee guida 4/2019 sull'articolo 25 — Protezione dei dati fin dalla progettazione e per impostazione predefinita*, l'espressione misure tecniche e organizzative può essere intesa in senso lato come qualsiasi metodo o mezzo che un titolare del trattamento può impiegare nel trattamento. Con il termine "adeguate" si intende che le misure devono essere idonee a conseguire la finalità prevista, ossia devono attuare efficacemente i principi di protezione dei dati. L'obbligo di adeguatezza è quindi strettamente connesso a quello di efficacia[74].

[74] *Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita*, pag. 6, punto 8.

ii. Sospendere l'account

167. In alternativa, agli utenti è offerta la possibilità di disattivare temporaneamente il proprio account, ossia di abbandonare i social media per un certo periodo di tempo senza cancellare definitivamente l'account. In questo caso l'account è temporaneamente disattivato e il profilo, le immagini, i commenti e le reazioni saranno nascosti fino a quando gli utenti non riattivano il proprio account, ad esempio accedendovi nuovamente. La principale differenza rispetto alla cancellazione è che i dati personali rimangono presso il social network e che l'account può essere riattivato dagli utenti senza una nuova registrazione.

168. Gli utenti che iniziano il processo di cancellazione del loro account potrebbero trovare già preselezionata l'opzione di sospensione dell'account. Anche se l'offerta di un'opzione di sospensione potrebbe risultare utile per gli utenti che non ancora desiderano cancellare definitivamente il loro account, i fornitori di social media non possono imporre simili periodi di riflessione agli utenti, in particolare attraverso funzioni preselezionate. Offrendo la possibilità di disattivazione, il fornitore di social media crea nell'utente la ragionevole aspettativa che i suoi dati personali non saranno trattati come durante l'uso attivo dell'account e che durante tale periodo il fornitore di social media ridurrà il trattamento dei dati personali a un livello strettamente necessario. L'utente potrebbe aspettarsi che i suoi dati non siano trattati per finalità specifiche o lo siano solo in parte, ad esempio migliorando il suo profilo con visite a siti web di terzi che utilizzano strumenti di targeting o tracciamento adeguati. Oltre a informare l'utente in modo trasparente in merito alle conseguenze della sospensione del suo account, qualsiasi trattamento dei dati effettuato durante la sospensione deve basarsi su una base giuridica valida.

169. Per quanto riguarda il trattamento dei dati basato sul consenso a norma dell'articolo 6, paragrafo 1, lettera a), GDPR, il fornitore di social media deve tenere conto del fatto che gli utenti si aspettano che il consenso prestato durante la registrazione o successivamente riguardi solo il trattamento dei dati durante l'utilizzo attivo dell'account. L'EDPB riconosce che la durata del consenso dipende dal contesto, dalla portata del consenso originale e dalle aspettative dell'interessato[75]. Sebbene il GDPR non preveda alcun termine specifico per la durata del consenso, la validità dipenderà dal contesto, dalla portata del consenso originale e dalle aspettative dell'interessato[76]. Se i trattamenti cambiano o si evolvono in maniera considerevole, il consenso originale non è più valido[77]. Come migliore prassi l'EDPB raccomanda di aggiornare il consenso a intervalli appropriati[78]. Fornire nuovamente tutte le informazioni contribuisce a garantire che l'interessato rimanga ben informato su come vengono utilizzati i suoi dati e su come può esercitare i suoi diritti[79]. In tal caso, occorrerà un nuovo consenso[80] e devono essere soddisfatti tutti i requisiti corrispondenti.

170. Nell'applicazione dell'articolo 6, paragrafo 1, lettera f), GDPR si dovrebbe tenere conto anche delle ragionevoli aspettative dell'interessato (cfr. considerando 47 del GDPR). In particolare, occorre valutare l'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli utenti tuttavia si aspettano ragionevolmente che durante il periodo di disattivazione il trattamento avrà luogo solo nella misura necessaria. Inoltre il fornitore di social media può invocare un interesse legittimo solo se sono soddisfatte tutte le fasi della valutazione dell'interesse legittimo, compreso il test comparativo.

[75] Linee guida 5/2020 sul consenso, punto 110.
[76] Linee guida 5/2020 sul consenso, punto 110.
[77] Linee guida 5/2020 sul consenso, punto 110.
[78] Linee guida 5/2020 sul consenso, punto 111.
[79] Linee guida 5/2020 sul consenso, punto 111.
[80] Cfr. Linee guida 5/2020 sul consenso, punto 110.

Eventuali interessi prevalenti o diritti e libertà fondamentali dell'interessato dovrebbero essere valutati caso per caso.

171. Dato che durante la disattivazione è sospesa anche gran parte degli obblighi contrattuali, le operazioni di trattamento dei dati di cui all'articolo 6, paragrafo 1, lettera b), GDPR sono necessarie solo in misura limitata. Può essere considerata necessaria solo la conservazione dei dati degli utenti fino alla decisione definitiva di riattivazione o di cancellazione.

172. In considerazione del fatto che tutti i precedenti trattamenti di dati erano mirati a un account attivo, se non sono incluse nelle informazioni generali di cui agli articoli 13 e 14 GDPR, devono essere fornite informazioni supplementari sul trattamento durante la disattivazione. Ciò deriva dai principi di trasparenza e correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR e dalla limitazione delle finalità di cui all'articolo 5, paragrafo 1, lettera b), GDPR. Il trattamento dei dati a seguito della disattivazione deve essere accompagnato dalla fornitura di informazioni sufficienti all'interessato. Pertanto il fornitore di social media informa in modo esauriente gli utenti in merito al trattamento effettivo e alle sue finalità durante la sospensione e, se necessario, ottiene un nuovo consenso.

b. Modelli di progettazione ingannevoli

i. Modelli basati sui contenuti

Overloading — Privacy intricata (lista di controllo 4.1.2 dell'allegato I)

173. In questo caso d'uso il modello di progettazione ingannevole della ***privacy intricata*** si verifica quando gli utenti sono sommersi da una quantità di informazioni distribuite in più spazi con l'intento di impedire loro di cancellare il proprio account, come illustrato nell'esempio che segue. Sebbene alcune informazioni supplementari prima di questa fase siano piuttosto auspicabili, come l'indicazione che gli utenti hanno accesso ai loro dati prima della cancellazione, le informazioni generali non correlate non sono più essenziali e l'azione dell'utente non dovrebbe essere immotivatamente rallentata.

> **Example 52:** L'utente è alla ricerca del diritto alla cancellazione. Per trovare un link alla cancellazione dell'account deve accedere alle impostazioni dell'account, aprire il sottomenu "privacy" e scorrerlo fino in fondo.

Stirring — Stimolazione emotiva (lista di controllo 4.3.1 dell'allegato I)

> **Example 53:** Nel primo livello di informazione l'utente riceve informazioni che evidenziano unicamente le conseguenze negative e scoraggianti della cancellazione del suo account (ad esempio "*perderai per sempre tutti i contenuti*" o "*i tuoi amici si dimenticheranno di te*").

174. Sebbene il rammarico per la cessazione del rapporto contrattuale appaia adeguato sotto il profilo sociale e sia quindi difficile da inquadrare in termini giuridici, una descrizione completa delle conseguenze asseritamente negative causate dalla cancellazione dell'account da parte dell'utente costituisce un ostacolo alla sua decisione se è presentata come nell'esempio precedente, che fa leva sulla paura di essere tagliati fuori (*Fear of Missing out*), rendendo particolarmente punitiva la scelta di cancellare il proprio account. Questo tipo di ***stimolazione emotiva*** dell'utente, consistente nel prospettargli che, se chiuderà l'account, resterà solo, costituisce una violazione dell'obbligo di agevolare l'esercizio dei diritti dell'interessato ai sensi dell'articolo 12, paragrafo 2, GDPR, nonché del principio di correttezza di cui all'articolo 5, paragrafo 1, lettera a), GDPR.

Left in the dark — Formulazioni o informazioni ambigue (lista di controllo 4.6.3 dell'allegato I)

175. Nel contesto della cancellazione di un account di social media, gli utenti possono trovarsi di fronte anche al modello di progettazione ingannevole delle ***formulazioni o informazioni ambigue***, illustrato negli esempi seguenti.

> **Example 54:** Quando gli utenti cancellano il proprio account, non viene loro comunicato per quanto tempo i loro dati saranno conservati dopo la cancellazione. Cosa ancora peggiore, in nessun momento del processo di cancellazione gli utenti sono avvisati del fatto che "*alcuni dati personali*" potrebbero essere conservati anche dopo l'eliminazione dell'account, ma devono ricercare da sé questa informazione nelle diverse fonti informative disponibili.
>
> **Example 55:** Gli utenti possono cancellare il proprio account unicamente attraverso link denominati *"Arrivederci"* o *"Disattiva"* disponibili nell'account stesso.

176. In questi esempi, la formulazione utilizzata per i link non indica chiaramente il fatto che gli utenti saranno reindirizzati al processo di cancellazione dell'account. Al contrario, è probabile che gli utenti pensino ad altre funzionalità, quali la disconnessione fino al successivo utilizzo o la disattivazione del proprio account. Pertanto essa potrebbe essere interpretata come una violazione dell'articolo 12, paragrafo 2, GDPR, a norma del quale i titolari del trattamento dovrebbero agevolare l'esercizio dei diritti dell'interessato. Creando confusione nelle aspettative degli utenti associate al link, la piattaforma di social media non agevola pienamente l'esercizio del diritto di cancellazione. L'uso di tali termini ambigui in altri contesti potrebbe violare disposizioni del GDPR quali l'articolo 7 e, per analogia, l'articolo 17, paragrafo 1, lettera b), di tale regolamento.

ii. Modelli basati sull'interfaccia

Skipping — Comodità ingannevole (lista di controllo 4.2.1 dell'allegato I)

> **Example 56:** Nel processo di cancellazione del proprio account gli utenti possono scegliere tra due opzioni: eliminare il proprio account oppure sospenderlo. L'opzione di sospensione è selezionata per impostazione predefinita.

177. La prima opzione, ossia l'eliminazione dell'account, comporta la cancellazione di tutti i dati personali dell'utente, per cui la piattaforma di social media non è più in possesso di tali dati, fatta eccezione per quelli che rientrano nell'eccezione temporanea di cui all'articolo 17, paragrafo 3, GDPR. Al contrario, con la seconda opzione, ossia la sospensione dell'account, tutti i dati personali sono conservati e potenzialmente trattati dal fornitore di social media. Ciò comporta necessariamente maggiori rischi per l'interessato, ad esempio se si verifica una violazione dei dati e i dati ancora conservati dal fornitore di social media sono consultati, duplicati, trasferiti o altrimenti trattati. La selezione predefinita dell'opzione di sospensione potrebbe indurre gli utenti a scegliere tale opzione invece di eliminare il proprio account, come inizialmente desiderato. Pertanto la pratica descritta in questo esempio può essere considerata una violazione dell'articolo 12, paragrafo 2, GDPR, in quanto, nel caso di specie, non agevola l'esercizio del diritto alla cancellazione e tenta persino di indurre l'utente a non esercitarlo.

Skipping — Diversivo (lista di controllo 4.2.2 dell'allegato I)

178. Fornire agli utenti un mezzo per scaricare i propri dati quando comunicano la volontà di cancellare il proprio account può essere un'opzione pertinente. Infatti, una volta eliminato l'account, i dati

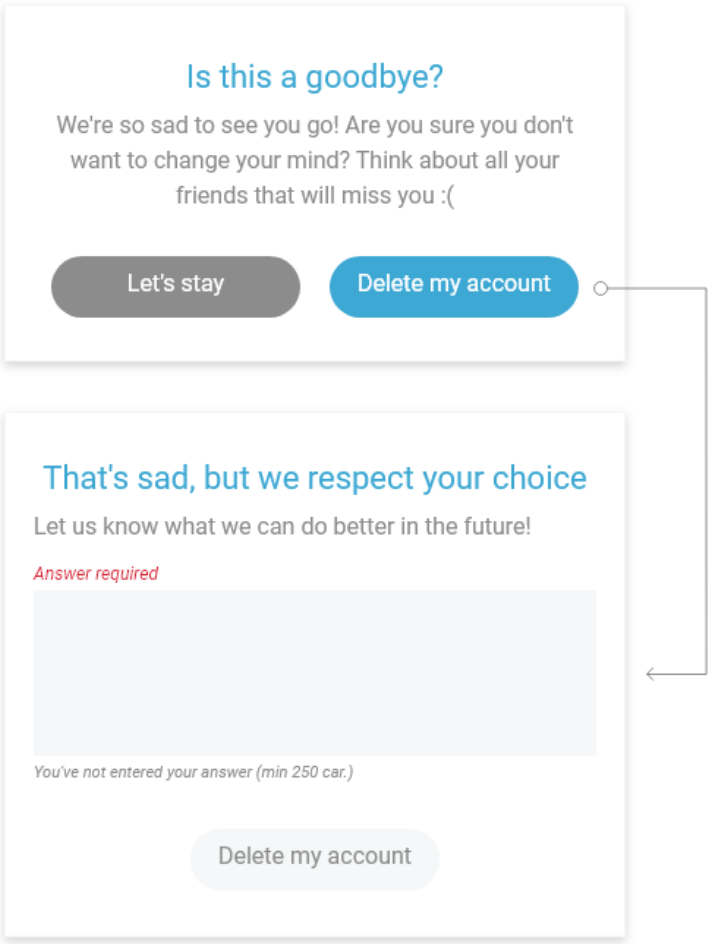
personali degli utenti saranno cancellati dopo un certo periodo di tempo. Ciò significa che gli utenti perderanno completamente tali dati personali se non ne ottengono una copia. La presentazione di questa opzione può tuttavia costituire un modello di progettazione ingannevole di ***diversivo***, come illustrato nell'esempio che segue.

> **Example 57:** Dopo aver cliccato su "Elimina il mio account", all'utente è offerta la possibilità di scaricare i propri dati, attuata come diritto alla portabilità, prima di eliminare l'account. Quando clicca per scaricare le proprie informazioni, l'utente è reindirizzato a una pagina di informazioni sul download. Tuttavia, una volta scelto quali dati scaricare e come scaricarli, l'utente non è reindirizzato al processo di eliminazione.

179. Nell'esempio di cui sopra, si potrebbe ritenere che le modalità di attuazione dell'opzione di download non agevolino l'esercizio del diritto alla cancellazione associato all'eliminazione dell'account. Infatti, una volta scaricati i propri dati, l'utente non è riportato al processo di eliminazione, ma potrà tornarvi solo con molti clic. Ostacolare in tal modo l'esercizio di un diritto viola l'articolo 12, paragrafo 2, GDPR. Inoltre è semplice realizzare una funzione che consenta all'utente di raggiungere facilmente il processo di eliminazione dopo aver scaricato i propri dati. A tale riguardo si potrebbe ritenere che l'obbligo di attuare misure tecniche e organizzative adeguate di cui all'articolo 25, paragrafo 1, GDPR, non sia rispettato in quanto gli utenti non sono in grado di continuare a esercitare efficacemente i propri diritti.

Obstructing — Allungare più del necessario (lista di controllo 4.4.2 dell'allegato I)

180. Come specificato nel caso d'uso n. 4, l'aggiunta di passaggi irrilevanti all'esercizio di un diritto potrebbero violare le disposizioni del GDPR, in particolare l'articolo 12, paragrafo 2. Tale considerazione si applica al momento in cui gli utenti intendono cancellare il loro account, in quanto il modello interferirebbe con il diritto alla cancellazione associato a tale richiesta.



Example 58: In questo esempio l'utente, dopo aver cliccato sul link o sul pulsante per cancellare il proprio account, visualizza innanzitutto una casella di conferma della cancellazione. Sebbene nella casella siano presenti alcuni elementi di ***stimolazione emotiva***, il passaggio può essere considerato una misura di sicurezza per evitare che l'utente elimini il proprio account cliccando per errore sul link. Tuttavia, quando clicca sul pulsante "Elimina il mio account", l'utente si trova di fronte a una seconda casella che gli chiede di descrivere con un testo il motivo per cui desidera chiudere l'account. Finché non inserisce qualcosa nella casella, non può eliminare il proprio account in quanto il pulsante associato all'azione è inattivo e grigio. Questa pratica ***allunga più del necessario*** la cancellazione di un account, in particolare dal momento che chiedere all'utente di produrre un testo che descriva il motivo per cui desidera lasciare un account richiede sforzi e tempo aggiuntivi e tale azione non dovrebbe essere obbligatoria per cancellare l'account.

181. Come osservato in precedenza, nell'esercizio di un diritto gli utenti non dovrebbero essere tenuti a rispondere a domande non connesse all'esercizio del diritto stesso. Il fatto di dover giustificare la propria scelta o spiegare in che modo la piattaforma di social media dovrebbe migliorare non risponde a tale principio. Nell'esempio illustrato, il problema è aggravato dal fatto che l'interessato, anziché selezionare una frase preformulata in un elenco, deve scrivere una risposta di sua completa creazione, il che richiede uno sforzo ancora maggiore. Questo meccanismo potrebbe escludere completamente alcuni utenti dall'esercizio del loro diritto, se non hanno abbastanza dimestichezza con la scrittura.

182. Tuttavia ciò non significa che un elenco di risposte preformulate sia un passaggio accettabile da aggiungere al processo di cancellazione di un account. Ciò vale in particolare se queste risposte sono associate a ulteriori passaggi e azioni imposte agli utenti, come dimostra l'esempio che segue.

> **Example 59:** Il fornitore di social media rende obbligatorio per gli utenti rispondere a una domanda sui motivi per cui desiderano cancellare il loro account selezionando la risposta tra quelle presenti un menu a tendina. Gli utenti hanno l'impressione che rispondere a questa domanda (in apparenza) consenta loro di realizzare l'azione desiderata, vale a dire eliminare l'account. Una volta selezionata una risposta, appare una finestra pop-up che mostra agli utenti un modo per risolvere il problema indicato nella loro risposta. Il processo domanda-risposta rallenta pertanto il processo di cancellazione dell'account da parte degli utenti.

183. Ad un una procedura di cancellazione dell'account resa particolarmente lunga si aggiunge un meccanismo di ***diversivo*** che mira a distogliere gli utenti dalla cancellazione del proprio account fornendo una soluzione alla loro motivazione alla base dell'uscita dalla piattaforma di social media. Tutto ciò ostacola l'esercizio del diritto alla cancellazione e, per analogia, dissuade gli interessati dall'esercitare il loro diritto.

Fickle - Decontestualizzazione (lista di controllo 4.5.2 dell'allegato I)

184. Infine, quando desiderano cancellare il proprio account, gli utenti possono incontrare anche il modello di progettazione ingannevole della ***decontestualizzazione***.

> **Example 60:** Sulla piattaforma di social media XY, il link per disattivare o cancellare l'account è disponibile nella scheda "*I tuoi dati XY*".

185. In generale i termini utilizzati come titolo di una pagina o di una sezione della piattaforma di social media dedicata alle questioni relative alla protezione dei dati dovrebbero riflettere chiaramente il tipo di informazioni o di controllo che vi sono contenuti. È improbabile che gli utenti medi colleghino le azioni per cancellare o disattivare il proprio account alla gestione dei dati. Nell'esempio precedente, gli utenti non si aspettano la funzionalità di cancellazione del loro account in una pagina denominata "I tuoi dati XY", che suggerisce la possibilità di consultare ed eventualmente modificare i propri dati. Cercherebbero invece una pagina "generale" o una pagina intitolata "Elimina il mio account". Pertanto, dal punto di vista degli utenti, le opzioni sono collocate in un contesto che è totalmente avulso e non corrisponde alle loro aspettative.

> **Example 61:** La scheda effettiva per cancellare un account figura nella sezione "*Elimina una funzione del tuo account*".

186. In questo esempio gli utenti potrebbero erroneamente interpretare il titolo della sezione come indicante semplicemente lo spazio in cui regolare le singole funzioni. Non si aspetterebbero pertanto di trovarvi l'opzione per eliminare l'intero account, il che rende loro difficile trovare il collegamento corretto per effettuare tale operazione.

187. Il modello di progettazione ingannevole della ***decontestualizzazione***, come illustrato nei due esempi precedenti, potrebbe essere considerato una violazione dell'articolo 12, paragrafo 2, GDPR, dato che gli utenti avrebbero difficoltà a trovare lo spazio giusto in cui esercitare il loro diritto alla cancellazione.

c. Migliori prassi

Formulazioni coerenti: per la definizione cfr. il caso d'uso n. 1 (pag. 22).
Fornitura di definizioni: per la definizione cfr. il caso d'uso n. 1 (pag. 22).
Uso di esempi: per la definizione cfr. il caso d'uso n. 1 (pag. 22).
Spiegazione delle conseguenze: per la definizione cfr. il caso d'uso n. 2c (pag. 32).
Coerenza tra i diversi dispositivi: per la definizione cfr. il caso d'uso n. 3a (pag. 39).

Per il Comitato europeo per la protezione dei dati

Il presidente

(Andrea Jelinek)

4 ALLEGATO I ELENCO DELLE CATEGORIE E DEI TIPI DI MODELLI DI PROGETTAZIONE INGANNEVOLI

L'elenco seguente fornisce una panoramica delle categorie di modelli di progettazione ingannevoli e dei tipi di modelli di progettazione ingannevoli all'interno di ciascuna categoria. Elenca inoltre le disposizioni del GDPR maggiormente interessate dai tipi di modelli di progettazione ingannevoli. I lettori dovrebbero tenere presente che, come indicato in precedenza, il principio del trattamento corretto di cui all'articolo 5, paragrafo 1, lettera a), GDPR costituisce un punto di partenza per valutare l'esistenza di modelli di progettazione ingannevoli. Si tratta di un principio trasversale e tutti i modelli di progettazione ingannevoli lo violerebbero, indipendentemente dal rispetto di altri principi di protezione dei dati[81].

Per ciascun modello, l'elenco contiene anche il numero degli esempi e il corrispondente caso d'uso (UC) per aiutare i lettori a trovarli rapidamente.

È importante osservare che tale elenco non è esaustivo e che modelli di progettazione ingannevoli possono pertanto verificarsi anche nei casi d'uso ai quali non corrisponde un esempio di modello di progettazione ingannevole nel testo delle linee guida.

4.1 *Overloading* (sovraccarico)

Gli utenti sono sommersi da una quantità di richieste, informazioni, opzioni o possibilità con l'intento di dissuaderli dal proseguire e di indurli a mantenere o accettare determinate pratiche in materia di dati.

4.1.1 *Continuous prompting* (sollecitazione continua)[82]

Gli utenti sono sollecitati a fornire più dati personali di quelli necessari per le finalità del trattamento o ad acconsentire a un altro uso dei propri dati, mediante ripetute richieste di fornire dati aggiuntivi o di prestare il consenso per una nuova finalità di trattamento. Tali ripetute sollecitazioni possono giungere attraverso uno o più dispositivi. È probabile che, stanchi di dover respingere la richiesta ogni volta che utilizzano la piattaforma dovendone interrompere l'utilizzo, gli utenti finiscano per cedere.

Disposizioni del GDPR interessate:

- *limitazione delle finalità: articolo 5, paragrafo 1, lettera b);*
- *consenso liberamente prestato: articolo 7* in combinato disposto con l'articolo 4, punto 11);
- *consenso specifico: articolo 7, paragrafo 2.*

Esempi: caso d'uso 1, esempi 1, 2; caso d'uso 3a esempio 34 (immagine).

[81] Cfr. sopra, punto 9 delle presenti linee guida.

[82] Questo modello è strettamente correlato a un tipo di modello denominato "*nagging*"(insistenza) presente nella letteratura accademica.

4.1.2 *Privacy Maze* (privacy intricata)

Si verifica quando determinate informazioni che gli utenti desiderano ottenere, un controllo specifico che desiderano utilizzare o un diritto dell'interessato che intendono esercitare risultano particolarmente difficili da individuare, in quanto, per ottenere l'informazione o il controllo in questione, gli utenti devono visitare un numero eccessivo pagine senza avere a disposizione una panoramica completa ed esaustiva. È probabile che gli utenti si arrendano o che non riescano a trovare le informazioni o il controllo pertinenti.

Disposizioni del GDPR interessate:

- *principio della trasparenza*: *articolo 5, paragrafo 1, lettera a), e informazioni trasparenti: articolo 12, paragrafo 1;*
- *principio della correttezza: articolo 5, paragrafo 1, lettera a);*
- *informazioni facilmente accessibili*: articolo 12, paragrafo 1;
- *facilità di accesso ai diritti*: articolo 12, paragrafo 2;
- *consenso informato*: articolo 7 in combinato disposto con l'articolo 4, punto 11).

Esempi: caso d'uso 2a, esempio 17; caso d'uso 3a, esempio 33; caso d'uso 3b, esempio 37; caso d'uso 4, esempi 47 (immagine) e 48 (immagine); caso d'uso 5, esempio 51.

4.1.3 *Too many options* (troppe opzioni)

Consiste nel fornire agli utenti (troppe) opzioni tra cui scegliere. La quantità di opzioni rende gli utenti incapaci di compiere una scelta o li porta a trascurare alcune impostazioni, soprattutto se le informazioni non sono disponibili. Alla fine ciò può indurli a rinunciare o a tralasciare le impostazioni delle proprie preferenze in materia di dati personali e i propri diritti.

Disposizioni del GDPR interessate:

- *principi di trasparenza e correttezza:* articolo 5, paragrafo 1, lettera a);
- *informazioni trasparenti*: articolo 12, paragrafo 1.

Esempio: caso d'uso 3b, esempio 35.

4.2 *Skipping* (saltare)

Le interfacce o i percorsi utente sono progettati in modo tale che gli utenti dimentichino del tutto o in parte gli aspetti legati alla protezione dei dati o non vi riflettano.

4.2.1 *Deceptive snugness* (comodità ingannevole)

Per impostazione predefinita, sono attivate le funzioni e le opzioni più invasive. Per via dell'effetto default, che induce le persone a mantenere un'opzione preselezionata, è improbabile che gli utenti modifichino questo aspetto anche se ne hanno la possibilità.

Disposizioni del GDPR interessate:

- *protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita*: articolo 25, paragrafo 1;

- *consenso:* articolo 4, punto 11), e articolo 6 (pratica illecita di attivare un trattamento basato sul consenso per impostazione predefinita).

Esempi: caso d'uso 1, esempio 9; caso d'uso 3b, esempi 39 e 40 (immagine); caso d'uso 5, esempio 55.

4.2.2 *Look over there* (diversivo)

Un'azione o un'informazione relativa alla protezione dei dati è messa in concorrenza con un altro elemento che può essere collegato o meno alla protezione dei dati. È probabile che gli utenti che scelgono l'opzione posta come diversivo finiscano per trascurare l'altra, anche se questa costituiva il loro primo obiettivo.

Disposizioni del GDPR interessate:

- *principi di trasparenza e correttezza:* articolo 5, paragrafo 1, lettera a);
- *informazioni trasparenti*: articolo 12, paragrafo 1;
- *esercizio dei diritti:* articolo 12, paragrafo 2.

Esempi: caso d'uso 2c, esempio 25; caso d'uso 3a, esempio 29; caso d'uso 5, esempi 56 e 58.

4.3 *Stirring* (infondere agitazione)

Le scelte degli utenti sono influenzate facendo leva sulle loro emozioni o utilizzando sollecitazioni visive.

4.3.1 *Emotional Steering* (stimolazione emotiva)[83]

Consiste nell'utilizzare una formulazione o elementi visivi (ad esempio stile, colori, immagini o altro) in modo da trasmettere le informazioni agli utenti in una prospettiva molto positiva che li fa sentire bene, al sicuro o ricompensati, o molto negativa, che li fa sentire spaventati, colpevoli o puniti. Influenzare lo stato emotivo degli utenti in questo modo può indurli ad agire contro i loro interessi in materia di protezione dei dati.

Disposizioni del GDPR interessate:

- *principi di trasparenza e correttezza:* articolo 5, paragrafo 1, lettera a);
- *informazioni trasparenti*: articolo 12, paragrafo 1;
- *esercizio dei diritti:* articolo12, paragrafo 2;
- *consenso del minore:* articolo 8;
- *consenso informato*: articolo 7, in combinato disposto con l'articolo 4, punto 11);

Esempi: caso d'uso 1, esempi 4, 5, 6; caso d'uso 5, esempio 52.

[83]Tale modello è strettamente correlato a un tipo di modello denominato "*Toying with Emotions*" (giocare con le emozioni) riscontrato, tra l'altro, nelle relazioni di organizzazioni intergovernative quali la Commissione europea, Direzione generale della Giustizia e dei consumatori, Lupiáñez-Villanueva, F., Boluda, A., Bogliacino, F., et al., *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation: final report*, Ufficio delle pubblicazioni dell'Unione europea, 2022, https://data.europa.eu/doi/10.2838/859030 e OCSE (2022), "Dark commercial patterns", *Documents de travail de l'OCDE sur l'économie numérique*, n. 336, Edizioni OCDE, Parigi, https://doi.org/10.1787/44f5e846-en.

4.3.2 *Hidden in plain sight* (poca visibilità)

Consiste nell'utilizzare uno stile visivo o una tecnica per controllare le informazioni o la protezione dei dati che porti gli utenti a scegliere opzioni meno restrittive e quindi più invasive.

Disposizioni del GDPR interessate:

- *principio della correttezza*: articolo 5, paragrafo 1, lettera a);
- *consenso liberamente prestato:* articolo 7 in combinato disposto con l'articolo 4, punto 11);
- *informazioni chiare*: articolo 12, paragrafo 1;
- *esercizio dei diritti:* articolo12, paragrafo 2

Esempi: caso d'uso 1, esempio 8, caso d'uso 3a esempio 34 (immagine); caso d'uso 3b, esempio 40 (immagine); caso d'uso 4, esempio 48.

4.4 *Obstructing* (creazione di ostacoli)[84]

Consiste nell'ostacolare o bloccare gli utenti nel processo di ottenimento di informazioni o di gestione dei loro dati rendendo difficile o impossibile la sua realizzazione.

4.4.1 *Dead end* (punto morto)

Gli utenti cercano informazioni o un controllo, ma non riescono a trovarli in quanto un collegamento di reindirizzamento non funziona o non è disponibile. Gli utenti non sono messi in condizione di raggiungere il loro scopo.

Disposizioni del GDPR interessate:

- *informazioni facilmente accessibili*: articolo 12, paragrafo 1;
- *esercizio dei diritti*: articolo 12, paragrafo 2;
- *protezione dei dati fin dalla progettazione e la protezione per impostazione predefinita*: articolo 25, paragrafo 1.

Esempi: caso d'uso 1, esempi 10, 11; caso d'uso 2a, esempio 18; caso d'uso 3a, esempi 30, 31; caso d'uso 4, esempio 43.

4.4.2 *Longer than necessary* (allungare più del necessario)

Quando gli utenti cercano di attivare un controllo relativo alla protezione dei dati, il percorso utente è impostato in modo da richiedere il completamento di un numero di passaggi superiore rispetto a quello necessario per l'attivazione di scelte invasive riguardo ai dati. Ciò potrebbe dissuaderli dall'attivare tale controllo.

[84] Questa categoria è strettamente correlata alla strategia denominata "*Obstruction*" definita e descritta in Gray Colin M., Kou Yubo, Battles Bryan, Hoggatt Joseph e Toombs Austin L. 2018. *The Dark (Patterns) Side of UX Design*, Atti della conferenza CHI del 2018 "Human Factors in Computing Systems" (Montreal QC, Canada) (CHI' 18). ACM, New York, NY, USA, articolo 534, 14 pagine. https://doi.org/10.1145/3173574.3174108.

Disposizioni del GDPR interessate:

- *informazioni facilmente accessibili*: articolo 12, paragrafo 1;
- *esercizio dei diritti*: articolo 12, paragrafo 2;
- *diritto di opposizione*: articolo 21, paragrafo 1;
- *revoca del consenso*: articolo 7, paragrafo 3;
- *protezione dei dati fin dalla progettazione (e per impostazione predefinita)*: articolo 25, paragrafo 1.

Esempi: caso d'uso 1, esempio 7; caso d'uso 3a, esempio 32; caso d'uso 4, esempio 50; caso d'uso 5, esempi 57 (immagine) e 58.

4.4.3 *Misleading action* (azione ingannevole)

Una discrepanza tra le informazioni e le azioni a disposizione degli utenti li induce a compiere un'operazione non voluta. La differenza tra ciò che gli utenti si aspettano e ciò che ottengono rischia di dissuaderli dal proseguire.

Disposizioni del GDPR interessate:

- *informazioni trasparenti*: articolo 12, paragrafo 1;
- *correttezza del trattamento*: articolo 5, paragrafo 1, lettera a).
- *consenso informato*: articolo 7, paragrafo 2, in combinato disposto con l'articolo 4, punto 11).

Esempi: caso d'uso 1, esempio 3; caso d'uso 3a, esempio 28.

4.5 *Fickle* (ambiguità)

La progettazione dell'interfaccia è incerta e incoerente, il che rende difficile per gli utenti individuare la natura del trattamento, operare una scelta adeguata per quanto riguarda i loro dati e individuare dove si trovano i diversi controlli.

4.5.1 *Lacking hierarchy* (mancanza di gerarchia)

Le informazioni relative alla protezione dei dati non hanno una gerarchia, compaiono più volte e sono presentate in modi diversi. È probabile che gli utenti siano confusi da tale ridondanza e non siano in grado di comprendere appieno le modalità con cui i loro dati sono trattati né come esercitare il controllo su di essi.

Disposizioni del GDPR interessate:

- *informazioni facilmente accessibili*: articolo 12, paragrafo 1;
- *esercizio dei diritti: articolo 12, paragrafo 2.*

Esempi: caso d'uso 2a, esempi 13 e 14.

4.5.2 *Decontextualising* (decontestualizzazione)

Un'informazione o un controllo sulla protezione dei dati si trova su una pagina che è slegata dal contesto. È improbabile che gli utenti trovino le informazioni o il controllo in quanto non sarebbe intuitivo cercarli su quella pagina.

Disposizioni del GDPR interessate:

- *informazioni facilmente accessibili*: articolo 12, paragrafo 1;
- *informazioni trasparenti*: articolo 12, paragrafo 1;
- *esercizio dei diritti: articolo 12, paragrafo 2.*

Esempi: caso d'uso 3b, esempi 41, 42; caso d'uso 5, esempi 59 e 60.

4.5.3 *Inconsistent interface* (interfaccia incoerente)

Un'interfaccia non è coerente nei diversi contesti (ad esempio, il menu relativo alla protezione dei dati non visualizza le stesse voci sul cellulare e sul desktop) o con le aspettative degli utenti (ad esempio, un'opzione si trova al posto di un'altra). Tali differenze possono far sì che gli utenti non trovino il controllo o le informazioni desiderati oppure che, per abitudine, interagiscano con un dato elemento dell'interfaccia anche se tale interazione li porta a compiere una scelta non voluta in materia di protezione dei dati.

Disposizioni del GDPR interessate:

- *informazioni facilmente accessibili*: articolo 12, paragrafo 1;
- *esercizio dei diritti: articolo 12, paragrafo 2.*

Esempi: caso d'uso 3b, esempio 39; caso d'uso 4, esempio 50.

4.5.4 *Language discontinuity* (discontinuità linguistica)

Le informazioni relative alla protezione dei dati non sono fornite in una lingua ufficiale del paese in cui vivono gli utenti, mentre il servizio è fornito in tale lingua. Se non padroneggiano la lingua in cui sono fornite le informazioni sulla protezione dei dati, gli utenti non saranno in grado di leggerle facilmente e pertanto non saranno a conoscenza delle modalità di trattamento dei dati.

Disposizioni del GDPR interessate:

- *correttezza del trattamento*: articolo 5, paragrafo 1, lettera a);
- *informazioni intelligibili*: articolo 12, paragrafo 1, articolo 13 e articolo 14;
- *uso di un linguaggio chiaro e semplice per le informazioni*: articolo 12, paragrafo 1, articolo 13 e articolo 14.

Esempi: caso d'uso 2a, esempio 16; caso d'uso 3a, esempi 26 (immagine) e 27; caso d'uso 4, esempio 44.

4.6 *Left in the dark (lasciare all'oscuro)*

L'interfaccia è progettata in modo da nascondere informazioni o controlli relativi alla protezione dei dati o in modo da lasciare agli utenti nell'incertezza sulle modalità di trattamento dei loro dati e sul tipo di controlli che potrebbero avere su di essi.

4.6.1 *Conflicting information* (informazioni contrastanti)

Consiste nel fornire agli utenti informazioni in qualche modo contrastanti. È probabile che gli utenti non siano sicuri di come agire e di quali siano le conseguenze delle loro azioni, pertanto tenderanno a non intraprendere alcuna azione e a limitarsi a mantenere le impostazioni predefinite.

Disposizioni del GDPR interessate:

- *correttezza del trattamento*: articolo 5, paragrafo 1, lettera a);
- *informazioni trasparenti*: articolo 12, paragrafo 1;
- *consenso informato*: articolo 7, paragrafo 2, in combinato disposto con l'articolo 4, punto 11).

Esempi: caso d'uso 2a, esempio 12; caso d'uso 2c, esempio 20; caso d'uso 3b, esempio 36.

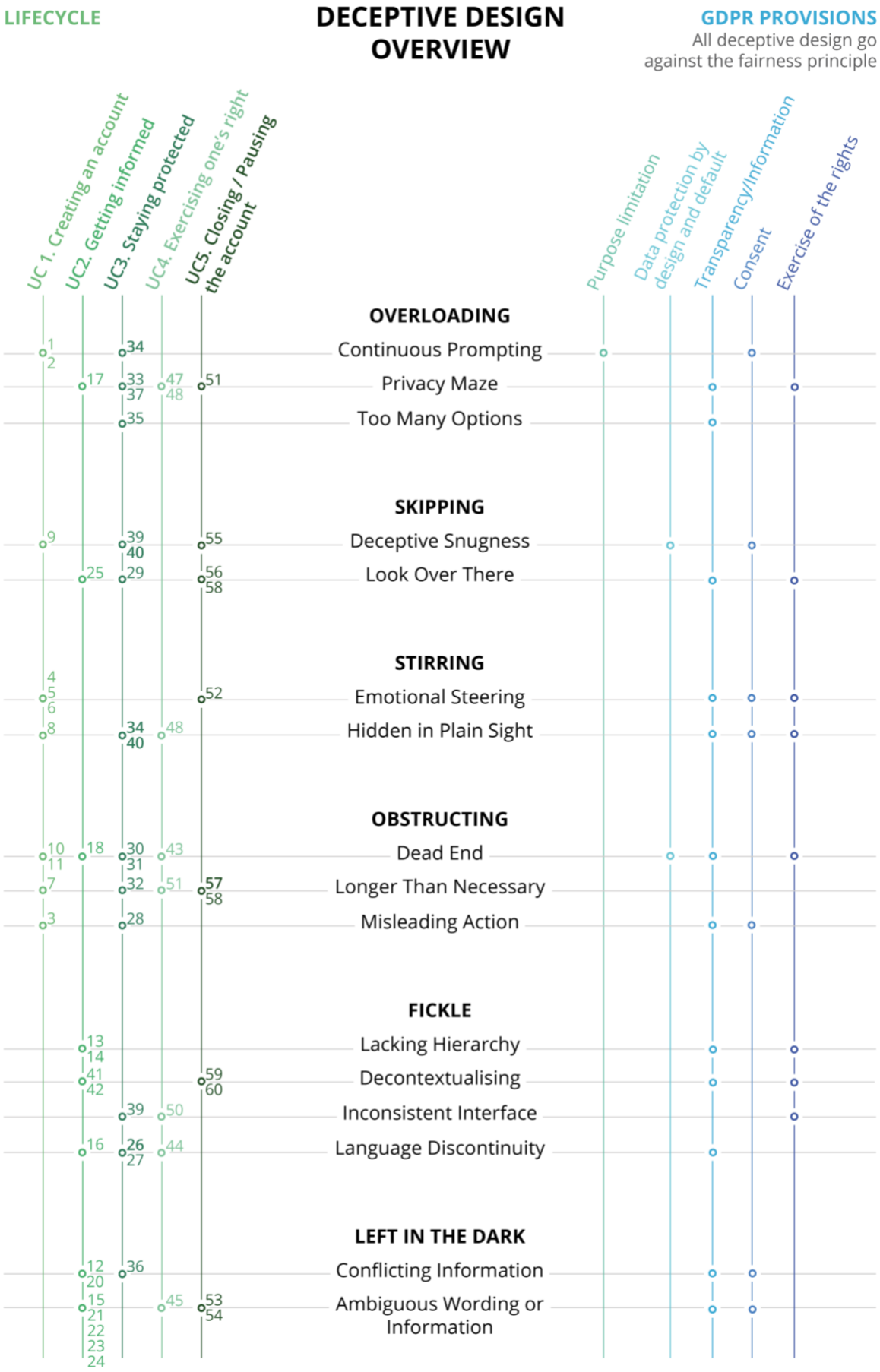
4.6.2 *Ambiguous wording or information* (formulazioni o informazioni ambigue)

Consiste nell'utilizzare termini ambigui e vaghi per fornire informazioni agli utenti. Gli utenti potrebbero essere incerti sulle modalità di trattamento dei dati o su come esercitare il controllo sui propri dati personali.

Disposizioni del GDPR interessate:

- *correttezza del trattamento*: articolo 5, paragrafo 1, lettera a);
- *informazioni trasparenti*: articolo 12, paragrafo 1;
- *uso di un linguaggio chiaro e semplice per le informazioni*: articolo 12, paragrafo 1;
- *consenso informato*: articolo 7, paragrafo 2, in combinato disposto con l'articolo 4, punto 11);
- *informazioni incomplete*: articolo 13
- *disposizioni specifiche a seconda del particolare caso d'uso*, ad esempio l'articolo 34 *per il caso d'uso 2c*.

Esempi: caso d'uso 2a, esempio 15; caso d'uso 2c, esempi 21, 22, 23, 24; caso d'uso 4, esempio 45; caso d'uso 5, esempi 53 e 54.


LIFECYCLE
DECEPTIVE DESIGN OVERVIEW
GDPR PROVISIONS
All deceptive design go against the fairness principle
UC 1. Creating an account
UC2. Getting informed
UC3. Staying protected
UC4. Exercising one's right
UC5. Closing / Pausing the account
Purpose limitation
Data protection by design and default
Transparency/Information
Consent
Exercise of the rights
OVERLOADING
Continuous Prompting
Privacy Maze
Too Many Options
SKIPPING
Deceptive Snugness
Look Over There
STIRRING
Emotional Steering
Hidden in Plain Sight
OBSTRUCTING
Dead End
Longer Than Necessary
Misleading Action
FICKLE
Lacking Hierarchy
Decontextualising
Inconsistent Interface
Language Discontinuity
LEFT IN THE DARK
Conflicting Information
Ambiguous Wording or Information

5 ALLEGATO II: MIGLIORI PRASSI

Il seguente elenco fornisce una panoramica delle migliori prassi descritte nelle linee guida alla fine di ciascun caso d'uso, che possono essere utilizzate per progettare interfacce utente che facilitino l'efficace attuazione del GDPR. Tali migliori prassi possono rappresentare un primo passo verso un modo standardizzato per consentire agli utenti di controllare efficacemente i loro dati e di esercitare i loro diritti.

Scorciatoie: i link a informazioni, azioni o impostazioni che possono essere di aiuto pratico agli utenti nella gestione dei loro dati e delle loro impostazioni di protezione dei dati dovrebbero essere disponibili ogni qualvolta gli utenti si trovino di fronte a informazioni o esperienze correlate a tali aspetti (*ad esempio link che reindirizzano alle parti pertinenti della politica sulla privacy*). *ad esempio, nella politica sulla privacy, per ogni informazione sulla protezione dei dati fornire link che reindirizzano direttamente alle relative pagine sulla protezione dei dati sulla piattaforma di social media; fornire agli utenti un link per reimpostare la loro password*; *quando sono informati su un aspetto del trattamento, gli utenti sono invitati a impostare le loro preferenze riguardo ai dati sulla corrispondente pagina delle impostazioni/nel pannello di controllo; fornire un link alla cancellazione dell'account nell'account utente*)**.**

Raggruppamento di opzioni: riunire opzioni che hanno la stessa finalità di trattamento in modo che gli utenti possano modificarle più facilmente, pur lasciando agli utenti stessi la possibilità di apportare modifiche più granulari. Se le piattaforme di social media presentano raggruppamenti di opzioni, queste non dovrebbero contenere elementi imprevisti o non correlati (ad esempio elementi con finalità diverse). Se il trattamento è subordinato al consenso, i raggruppamenti di opzioni devono essere in linea con le linee guida dell'EDPB sul consenso, in particolare i punti da 42 a 44.

Informazioni di contatto: l'indirizzo di contatto della società a cui inviare le richieste di protezione dei dati dovrebbe essere chiaramente indicato nella politica sulla privacy. Dovrebbe essere presente in una sezione in cui gli utenti possono aspettarsi di trovarlo, ad esempio una sezione sull'identità del responsabile del trattamento dei dati, una sezione relativa ai diritti o una dedicata ai contatti.

Indicazioni per contattare l'autorità di controllo: indicare l'identità specifica dell'autorità di controllo e includere un link al suo sito web o alla pagina web specifica relativa alla presentazione di un reclamo. Tali informazioni dovrebbero essere presenti in una sezione in cui gli utenti possono aspettarsi di trovarle, ad esempio una sezione relativa ai diritti.

Panoramica della politica sulla privacy: all'inizio/nella parte superiore della pagina della politica sulla privacy, includere un indice (a tendina) con voci e sottovoci che mostri le diverse sezioni contenute nell'informativa sulla privacy. I nomi delle singole sezioni indicano chiaramente agli utenti l'esatto contenuto delle stesse, consentendo loro di individuare rapidamente la sezione desiderata e di accedervi.

Individuazione e confronto delle modifiche: quando sono apportate modifiche all'informativa sulla privacy, rendere accessibili le versioni precedenti con la relativa data di pubblicazione ed evidenziare le modifiche.

Formulazioni coerenti: in tutto il sito web sono utilizzate le stesse parole e la stessa definizione per un determinato aspetto della protezione dei dati. Le espressioni utilizzate nella politica sulla privacy dovrebbero corrispondere a quelle utilizzate sul resto della piattaforma.

Fornitura di definizioni: quando si utilizzano parole o un gergo non familiari o tecnici, fornire una definizione in un linguaggio semplice aiuterà gli utenti a comprendere le informazioni loro comunicate. La definizione può essere riportata direttamente nel testo, comparendo quando l'utente passa il cursore sulla parola, come pure essere resa disponibile in un glossario.

Messa in evidenza degli elementi relativi alla protezione dei dati: rendere visivamente evidenti elementi o azioni collegati alla protezione dei dati in un'interfaccia non direttamente dedicata a tale aspetto. Ad esempio, quando si pubblica un messaggio pubblico sulla piattaforma, i controlli sull'associazione della geolocalizzazione dovrebbero essere direttamente disponibili e chiaramente visibili.

Protezione dei dati nella fase di *onboarding*: il fornitore di social media può includere nell'esperienza di *onboarding* immediatamente successiva alla creazione di un account una serie di momenti relativi alla protezione dei dati per consentire agli utenti di scoprire e impostare agevolmente le proprie preferenze. Può ad esempio invitarli a impostare le preferenze riguardo alla protezione dei dati dopo l'aggiunta del primo amico o la condivisione del primo post.

Uso di esempi: oltre alle informazioni obbligatorie che indicano in modo chiaro e preciso la finalità del trattamento, per illustrare un trattamento specifico dei dati e renderlo più concreto per gli utenti si possono utilizzare esempi.

Menu di navigazione "*sticky*" (fisso): durante la consultazione di una pagina relativa alla protezione dei dati, l'indice può rimanere costantemente visibile sullo schermo, in modo da consentire agli utenti di individuare la propria posizione nella pagina in ogni momento e di spostarsi rapidamente nel contenuto grazie a link di ancoraggio.

Inizio pagina: inserire in fondo alla finestra un pulsante che consente di tornare all'inizio della pagina o un elemento costantemente visibile sullo schermo che consente di spostarsi facilmente all'interno di una pagina.

Notifiche: le notifiche possono essere utilizzate per sensibilizzare gli utenti su aspetti, cambiamenti o rischi connessi al trattamento dei dati personali (ad esempio *in caso di violazione dei dati*). L'attuazione delle notifiche può avvenire in vari modi, ad esempio attraverso messaggi di posta in arrivo, finestre pop-in, banner fissi nella parte superiore della pagina web ecc.

Spiegazione delle conseguenze: se gli utenti desiderano attivare o disattivare un controllo della protezione dei dati o prestare o revocare il proprio consenso, informarli in modo neutro sulle conseguenze di tale azione.

Coerenza tra i diversi dispositivi: quando la piattaforma di social media è disponibile tramite dispositivi diversi (ad esempio computer, smartphone ecc.), le impostazioni e le informazioni relative alla protezione dei dati dovrebbero essere situate negli stessi spazi nelle diverse versioni e dovrebbero essere accessibili attraverso lo stesso percorso e gli stessi elementi di interfaccia (menu, icone ecc.).

Directory della protezione dei dati: per facilitare l'orientamento attraverso le diverse sezioni del menu, fornire agli utenti una pagina facilmente accessibile dalla quale possano accedere a tutte le funzioni e informazioni relative alla protezione dei dati. La pagina si può trovare nel menu principale di navigazione del fornitore di social media, nell'account utente, attraverso la politica sulla privacy ecc.

Informazioni contestuali: oltre a un'esaustiva politica sulla privacy, fornire brevi informazioni nel momento più opportuno affinché l'utente resti costantemente e precisamente informato sulle modalità di trattamento dei propri dati.

Significato intuitivo dell'URL: le pagine relative alle impostazioni o alle informazioni sulla protezione dei dati dovrebbero utilizzare un indirizzo web che ne rifletta chiaramente il contenuto. Ad esempio una pagina che centralizza il controllo della protezione dei dati potrebbe avere un URL del tipo [social-network.com]/impostazioni-dati.

Modulo per l'esercizio dei diritti: per agevolare gli utenti nell'esercizio dei propri diritti ai sensi del GDPR, fornire un modulo dedicato che li aiuti a comprendere i loro diritti e li guidi nella presentazione di questo tipo di richieste.