Regolamento generale sulla protezione dei dati

"GDPR" reindirizza qui.

Regolamento (UE) 2016/679	
Regolamento dell'Unione europea	
Titolo	Regolamento sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati e che abroga la direttiva 95/46 / CE (direttiva sulla protezione dei dati)
Fatto da	Parlamento europeo e Consiglio dell'Unione europea
Riferimento del giornale	L119, 4 maggio 2016, p. 1-88
Storia	
Data di realizzazione	14 aprile 2016
Data di attuazione	25 maggio 2018
Testi preparativi	
Proposta dellaCommissione	COM / 2012/010 def. - 2012/0010 (COD)
Altra legislazione	
Sostituisce	Direttiva sulla protezione dei dati
Legislazione attuale	

Il **regolamento generale sulla protezione dei dati** (UE) 2016/679 ("GDPR") è un regolamento nella legislazione dell'UE sulla protezione dei dati e sulla privacy per tutti gli individui all'interno dell'Unione europea (UE) e dello Spazio economico europeo(SEE). Affronta anche l'esportazione di dati personali al di fuori delle aree UE e SEE. Il GDPR mira principalmente a dare il controllo alle persone sui loro dati personali e a semplificare il contesto normativo per gli affari internazionali unificando il regolamento all'interno dell'UE. [1]

Sostituendo la direttiva 95/46 / CE sulla protezione dei dati , il regolamento contiene disposizioni e requisiti relativi al trattamento dei dati personali delle persone (formalmente denominati *soggetti dei dati* nel GDPR) all'interno dell'Unione europea e si applica a un'impresa stabilita nell'UE o -Indipendentemente dalla sua ubicazione e dalla cittadinanza dei soggetti interessati, che sta elaborando i dati personali delle persone all'interno dell'UE. I *responsabili* del trattamento dei dati personali devono *adottare misure tecniche e organizzative adeguate* per attuare i principi di protezione dei dati.

"Protezione dei dati in base alla progettazione e per impostazione predefinita", significa che i processi aziendali che gestiscono i dati personali devono essere progettati e costruiti tenendo conto dei principi e fornire salvaguardie per proteggere i dati (ad esempio utilizzando la pseudonimizzazione o la completa anonimizzazione, se del caso) e utilizzare il impostazioni di privacy più alte possibili per impostazione predefinita, in modo che i dati non siano disponibili pubblicamente senza consenso esplicito e informatoe non può essere utilizzato per identificare un soggetto senza ulteriori informazioni memorizzate separatamente. Nessun dato personale può essere trattato a meno che non sia fatto secondo una base legale specificata dal regolamento o a meno che il responsabile del trattamento o il responsabile del trattamento non abbia ricevuto un'affermazione univoca e individualizzata del consenso dell'interessato. L'interessato ha il diritto di revocare questo consenso in qualsiasi momento.

Un responsabile del trattamento dei dati personali deve divulgare chiaramente qualsiasi raccolta di dati , dichiarare le basi e le finalità legittime per l'elaborazione dei dati e indicare il periodo di conservazione dei dati e se è condivisa con terzi o al di fuori dell'UE. Gli interessati hanno il diritto di richiedere una copia portatile dei dati raccolti da un processore in un formato comune e il diritto di cancellare i propri dati in determinate circostanze. Le autorità pubbliche e le imprese le cui attività principali sono incentrate sull'elaborazione regolare o sistematica dei dati personali, sono tenute ad assumere un *responsabile della protezione dei dati*(DPO), che è responsabile della gestione della conformità con il GDPR. Le aziende devono segnalare eventuali violazioni dei dati entro 72 ore se hanno un effetto negativo sulla privacy dell'utente.

Il GDPR è stato adottato il 14 aprile 2016 ed è diventato esecutivo a partire dal 25 maggio 2018. Poiché il GDPR è un regolamento, non una direttiva , non richiede che i governi nazionali approvino alcuna legislazione abilitante ed è direttamente vincolante ed applicabile. [*dubbioso - discutere*] In alcuni casi, i trasgressori del GDPR possono essere multati fino a 20 milioni di euro o fino al 4% del fatturato mondiale annuo dell'esercizio precedente nel caso di un'impresa, a seconda di quale sia maggiore.

Contenuto [modifica]

Struttura [modifica]

Il GDPR è composto da 99 *articoli* , raggruppati in 11 capitoli e 171 ulteriori *considerando* con osservazioni esplicative. I titoli dei capitoli sono:

- I - Disposizioni generali
- II - Principi
- III - Diritti dell'interessato
- IV - Controller e processore
- V - Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali
- VI - Autorità di controllo indipendenti
- VII - Cooperazione e coerenza
- VIII - Rimedi, responsabilità e penalità
- IX - Disposizioni relative a specifiche situazioni di elaborazione
- X - Atti delegati e atti di esecuzione
- XI - Disposizioni finali

Scope [modifica]

Il regolamento si applica se il controllore dei dati (un'organizzazione che raccoglie dati dai residenti nell'UE) o il processore (un'organizzazione che elabora i dati per conto di un controllore dei dati come fornitori di servizi cloud) o l'interessato (persona) ha sede nell'UE . In determinate circostanze, [2] il regolamento si applica anche

alle organizzazioni con sede al di fuori dell'UE se raccolgono o trattano dati personali di individui situati all'interno dell'UE. Il regolamento non si applica al trattamento di dati da parte di una persona per "attività puramente personale o domestica e quindi senza alcuna connessione con un'attività professionale o commerciale". (Considerando 18)

Secondo la Commissione europea , "i dati personali sono tutte le informazioni relative a un individuo, che si riferiscano alla sua vita privata, professionale o pubblica. Può essere qualsiasi cosa, da un nome, un indirizzo di casa, una foto, un indirizzo email, dettagli bancari, post su siti web di social networking , informazioni mediche o indirizzo IP di un computer . " [3] Le definizioni precise di termini quali "dati personali", "trattamento", "soggetto dei dati", "responsabile del trattamento" e "incaricato del trattamento" sono indicate all'articolo 4 del regolamento [4] .

Il regolamento non intende applicare al trattamento dei dati personali per le attività di sicurezza nazionale o l'applicazione della legge dell'UE; tuttavia, i gruppi industriali preoccupati di fronte a un potenziale conflitto di leggi si sono chiesti se l'articolo 48 [5] del GDPR potrebbe essere invocato per cercare di impedire a un responsabile del trattamento dati soggetto alle leggi di un paese terzo di ottemperare a un ordine giuridico da parte delle forze dell'ordine di quel paese autorità giudiziarie o di sicurezza nazionale per divulgare a tali autorità i dati personali di una persona dell'UE, indipendentemente dal fatto che i dati risiedano dentro o fuori dell'UE. L'articolo 48 stabilisce che qualsiasi sentenza di un tribunale o tribunalee qualsiasi decisione di un'autorità amministrativa di un paese terzo che richieda a un responsabile del trattamento oa un responsabile di trasferire o divulgare dati personali può non essere riconosciuta o attuabile in alcun modo se non sulla base di un accordo internazionale, come un trattato di mutua assistenza giudiziaria in vigore tra il terzo richiedente (non UE) paese e l'UE o uno stato membro. Il pacchetto di riforma sulla protezione dei dati comprende anche una direttiva sulla protezione dei dati separata per il settore della polizia e della giustizia penale [6] che fornisce norme sugli scambi di dati personali a livello nazionale, europeo e internazionale.

Un unico insieme di regole si applicherà a tutti gli stati membri dell'UE. Ciascuno Stato membro istituirà un'autorità di vigilanza indipendente (SA) per ascoltare e indagare sui reclami, sanzionare i reati amministrativi, ecc. Le SA in ogni stato membro coopereranno con altre SA, fornendo assistenza reciproca e organizzando operazioni congiunte. Se un'azienda ha più stabilimenti nell'UE, avrà un'unica SA come "autorità capofila", in base all'ubicazione del suo "stabilimento principale" in cui si svolgono le principali attività di trattamento. L'autorità capofila fungerà da " sportello unico " per sorvegliare tutte le attività di trattamento di tale impresa in tutta l'UE [7] [8] (articoli 46-55 del GDPR). Un consiglio europeo per la protezione dei dati(EDPB) coordinerà le SA. L'EDPB sostituirà il gruppo di lavoro sulla protezione dei dati ai sensi dell'articolo 29 . Esistono eccezioni per i dati trattati in un contesto lavorativo o in sicurezza nazionale che potrebbero ancora essere soggetti alle normative nazionali (articolo 2 (2) (a) e 88 del GDPR).

Base legale per l'elaborazione [modifica]

A meno che l'interessato non abbia fornito il consenso informato al trattamento dei dati per uno o più scopi, i dati personali non possono essere trattati a meno che non vi sia almeno una base legale per farlo. Ai sensi dell'articolo 6, gli scopi legittimi sono: [9]

- (a) se l'interessato ha acconsentito al trattamento dei propri dati personali;
- (b) per adempiere agli obblighi contrattuali con una persona interessata, o per compiti su richiesta di una persona interessata che sta per concludere un contratto;
- (c) per rispettare gli obblighi legali di un responsabile del trattamento;
- (d) proteggere gli interessi vitali di un interessato o di un altro individuo;
- (e) svolgere un compito nell'interesse pubblico o in autorità ufficiale;
- (f) Per gli interessi legittimi di un responsabile del trattamento dei dati o di una terza parte, a meno che tali interessi non siano superati dagli interessi dell'interessato o dai suoi diritti in base alla Carta dei diritti fondamentali (in particolare nel caso dei minori).

Se il consenso informato viene utilizzato come base legale per il trattamento, il consenso deve essere esplicito per i dati raccolti e per i dati di ciascuna finalità utilizzati (articolo 7, definito all'articolo 4). Il consenso deve essere un'affermazione specifica, liberamente concessa, chiaramente formulata e inequivocabile fornita dall'interessato; un modulo online che ha opzioni di consenso strutturate come opt-out selezionate per impostazione predefinita è una violazione del GDPR, in quanto il consenso non è affermato in modo

inequivocabile dall'utente. Inoltre, più tipi di elaborazione non possono essere "raggruppati" insieme in un unico prompt di affermazione, in quanto ciò non è specifico per ciascun utilizzo dei dati e le singole autorizzazioni non vengono fornite liberamente. (Considerando 32)

Gli interessati devono poter ritirare questo consenso in qualsiasi momento e questo processo deve essere facile come in origine per l'opt-in. (Articolo 7, paragrafo 3) Un responsabile del trattamento non può rifiutare il servizio agli utenti che rifiutano il consenso al trattamento non è strettamente necessario per utilizzare il servizio. (Articolo 7, paragrafo 4) Consenso per i minori, definito nel regolamento come meno di 16 anni (sebbene con la possibilità per gli Stati membri di renderlo individualmente di 13 anni (articolo 8, paragrafo 1), [10] deve essere data dal genitore o custode del bambino e verificabile (articolo 8). [11]

Se il consenso al trattamento era già previsto dalla direttiva sulla protezione dei dati, il responsabile del trattamento dei dati non deve ottenere nuovamente il consenso se il trattamento è documentato e ottenuto in conformità ai requisiti del GDPR (considerando 171). [12]

Responsabilità e responsabilità [modifica]

Per essere in grado di dimostrare la conformità con il GDPR, il responsabile del trattamento dei dati deve attuare misure che soddisfino i principi di protezione dei dati in base alla progettazione e per impostazione predefinita. La protezione dei dati in base alla progettazione e per impostazione predefinita (articolo 25) richiede che le misure di protezione dei dati siano progettate nello sviluppo dei processi aziendali per prodotti e servizi. Tali misure comprendono la pseudonimizzazione dei dati personali, da parte del responsabile del trattamento, quanto prima possibile (considerando 78). È responsabilità e responsabilità del responsabile del trattamento dei dati applicare misure efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento anche se il trattamento è effettuato da un responsabile del trattamento per conto del responsabile del trattamento (considerando 74).

Una volta raccolti i dati, gli interessati devono essere chiaramente informati in merito alla portata della raccolta dei dati, alla base giuridica per il trattamento dei dati personali, alla durata dei dati, al trasferimento dei dati a una terza parte e / o al di fuori dell'UE, e divulgazione di qualsiasi processo decisionale automatizzato effettuato su base esclusivamente algoritmica . Ai soggetti di dati devono essere forniti i dettagli di contatto per il responsabile del trattamento e il loro responsabile designato della protezione dei dati, ove applicabile. I soggetti dei dati devono inoltre essere informati dei loro diritti alla privacy ai sensi del GDPR, compreso il loro diritto di revocare il consenso al trattamento dei dati in qualsiasi momento, il loro diritto di visualizzare i loro dati personali e accedere a una panoramica di come viene elaborato , il loro diritto di ottenere uncopia portatile dei dati memorizzati , il diritto alla cancellazione dei dati in determinate circostanze , il diritto di contestare qualsiasi processo decisionale automatizzato effettuato su base esclusivamente algoritmica e il diritto di presentare reclami presso l' autorità per la protezione dei dati . [13] [14]

Le valutazioni d'impatto sulla protezione dei dati (articolo 35) devono essere svolte quando si presentano rischi specifici per i diritti e le libertà degli interessati. È richiesta la valutazione e la mitigazione del rischio e per i rischi elevati è richiesta l'approvazione preventiva delle autorità per la protezione dei dati.

Protezione dei dati in base alla progettazione e per impostazione predefinita [modifica]

La protezione dei dati in base alla progettazione e per impostazione predefinita (articolo 25) richiede che la protezione dei dati sia progettata per lo sviluppo di processi aziendali per prodotti e servizi. Le impostazioni sulla privacy devono quindi essere impostate su un livello elevato per impostazione predefinita e le misure tecniche e procedurali devono essere adottate dal responsabile del trattamento per garantire che l'elaborazione, durante l'intero ciclo di vita della procedura, sia conforme al regolamento. I controllori dovrebbero anche implementare meccanismi per garantire che i dati personali non vengano elaborati se non necessario per ogni scopo specifico.

Un rapporto [15] da parte dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione elabora su ciò che deve essere fatto per ottenere privacy e protezione dei dati per impostazione predefinita. Specifica che le operazioni di crittografia e decrittografia devono essere eseguite localmente, non tramite il servizio remoto, poiché sia le chiavi che i dati devono rimanere nel potere del proprietario dei dati se si vuole raggiungere una certa privacy. Il report specifica che l'archiviazione di dati in outsourcing su cloud remoti è pratica e relativamente sicura se solo il proprietario dei dati, non il servizio cloud, detiene le chiavi di decrittografia.

Pseudonimizzazione [modifica]

Il GDPR si riferisce alla pseudonimizzazione come processo richiesto quando i dati sono archiviati (in alternativa all'altra opzione di completa anonimizzazione dei dati) [16] per trasformare i dati personali in modo tale che i dati risultanti non possano essere attribuiti a dati specifici soggetto senza l'uso di ulteriori informazioni. Un esempio è la crittografia , che rende i dati originali inintelligibili e il processo non può essere annullato senza l'accesso alla chiave di decrittografia corretta . Il GDPR richiede che le informazioni aggiuntive (come la chiave di decrittografia) siano conservate separatamente dai dati pseudonimizzati.

Un altro esempio di pseudonimizzazione è la tokenizzazione , che è un approccio non matematico alla protezione dei dati a riposo che sostituisce i dati sensibili con sostituti non sensibili, indicati come token. I token non hanno alcun significato o valore estrinseco o sfruttabile. La tokenizzazione non modifica il tipo o la lunghezza dei dati, il che significa che può essere elaborata da sistemi legacy come i database che potrebbero essere sensibili alla lunghezza e al tipo di dati.

Ciò richiede molte meno risorse computazionali da elaborare e meno spazio di archiviazione nei database rispetto ai dati crittografati tradizionalmente. Ciò si ottiene mantenendo i dati specifici completamente o parzialmente visibili per l'elaborazione e le analisi mentre le informazioni sensibili vengono tenute nascoste.

Si raccomanda la pseudonimizzazione per ridurre i rischi per gli interessati interessati e per aiutare i responsabili del trattamento e i responsabili del trattamento a rispettare i loro obblighi in materia di protezione dei dati (considerando 28). [17]

Diritto di accesso [modifica]

Il diritto di accesso (articolo 15) è un diritto dell'interessato. [18] Offre ai cittadini il diritto di accedere ai propri dati personali e informazioni su come questi dati personali vengono elaborati. Un responsabile del trattamento dei dati deve fornire, su richiesta, una panoramica delle categorie di dati oggetto di trattamento (articolo 15, paragrafo 1, lettera b), nonché una copia dei dati effettivi (articolo 15, paragrafo 3). Inoltre, il responsabile del trattamento dei dati deve informare l'interessato in merito al trattamento, come ad esempio le finalità del trattamento (articolo 15, paragrafo 1, lettera a)), con cui i dati sono condivisi (articolo 15, paragrafo 1, lettera c)) e in che modo ha acquisito i dati (articolo 15, paragrafo 1, lettera g)).

L'interessato deve essere in grado di trasferire i dati personali da un sistema di elaborazione elettronico a un altro, senza che ciò sia impedito dal responsabile del trattamento. I dati che sono stati sufficientemente anonimizzati sono esclusi, ma i dati che sono stati solo de-identificati ma rimane possibile il collegamento all'individuo in questione, ad esempio fornendo l'identificativo pertinente, non lo sono. [19] In pratica tuttavia fornire tali identificatori può essere difficile, come nel caso di Siri di Apple , in cui i dati vocali e di trascrizione sono archiviati con un identificativo personale che il produttore limita l'accesso a [20] o nel targeting comportamentale online, che fa molto affidamento sulle impronte digitali del dispositivopuò essere difficile catturare, inviare e verificare. [21]

Entrambi i dati vengono "forniti" dall'interessato e vengono inclusi i dati "osservati", come ad esempio il comportamento. Inoltre, i dati devono essere forniti dal controllore in un formato elettronico standard strutturato e comunemente usato. Il diritto alla portabilità dei dati è fornito dall'articolo 20 del GDPR. [22] Gli esperti legali vedono nella versione finale di questa misura un "nuovo diritto" creato che "va al di là dell'ambito della portabilità dei dati tra due controllori come previsto in [articolo 20]". [23]

Diritto alla cancellazione [modifica]

Un *diritto all'oblio è* stato sostituito da un più limitato *diritto di cancellazione* nella versione del GDPR adottata dal Parlamento europeo nel marzo 2014. [24] [25] L' articolo 17 stabilisce che l'interessato ha il diritto di chiedere la cancellazione dei dati personali ad essi connessi in base a una serie di motivi, tra cui la non conformità all'articolo 6, paragrafo 1 (legalità) che include il caso (f) se gli interessi legittimi del responsabile del trattamento sono superati dagli interessi o dai diritti e dalle libertà fondamentali dell'interessato, che richiedono la protezione dei dati personali (vedere anche *Google Spain SL, Google Inc., Agencia Española de Protección de Datos, Mario Costeja González*).

Registrazione delle attività di elaborazione [modifica]

Devono essere conservati registri delle attività di trattamento che includono finalità del trattamento, categorie coinvolte e limiti di tempo previsti. Le registrazioni devono essere messe a disposizione dell'autorità di controllo su richiesta (articolo 30). [26]

Responsabile della protezione dei dati [modifica]

Vedi anche: responsabile della protezione dei dati della Commissione europea

Se il trattamento è effettuato da un'autorità pubblica (ad eccezione dei tribunali o delle autorità giudiziarie indipendenti quando agiscono nell'esercizio delle loro funzioni giudiziarie), o se le operazioni di trattamento comportano un monitoraggio regolare e sistematico delle persone interessate su larga scala o se l'elaborazione su larga scala di categorie speciali di dati e dati personali relativi a condanne penali e reati (articolo 9 e articolo 10, [27]) un responsabile della protezione dei dati (DPO) - una persona con conoscenze specializzate in leggi e pratiche in materia di protezione dei dati - deve essere designato per controllore o incaricato del trattamento nel monitorare la conformità interna al regolamento.

Un responsabile della protezione dei dati designato può essere un membro del personale di un responsabile o un responsabile del trattamento oppure il ruolo può essere esternalizzato a una persona o agenzia esterna tramite un contratto di servizio. In ogni caso, l'organismo di elaborazione deve assicurarsi che non vi sia conflitto di interessi in altri ruoli o interessi che un responsabile della protezione dei dati può detenere. I dettagli di contatto per il responsabile della protezione dei dati devono essere pubblicati dall'organizzazione di trattamento (ad esempio, in una nota sulla privacy) e registrati presso l'autorità di vigilanza.

Il DPO è simile a un responsabile della conformità e dovrebbe anche essere esperto nella gestione dei processi IT, della sicurezza dei dati (compresa la gestione degli attacchi informatici) e di altri aspetti critici di continuità aziendale relativi alla gestione e all'elaborazione di dati personali e sensibili. Il set di competenze richiesto si estende oltre la comprensione della conformità legale alle leggi e ai regolamenti sulla protezione dei dati. Ulteriori dettagli sulla funzione e sul ruolo del responsabile della protezione dei dati sono stati forniti il 13 dicembre 2016 (rivisto il 5 aprile 2017) in un documento orientativo. [28]

Le organizzazioni con sede al di fuori dell'UE devono inoltre nominare una persona con sede nell'UE come rappresentante e punto di contatto per i loro obblighi GDPR (articolo 27). Si tratta di un ruolo distinto da un DPO, anche se esiste una sovrapposizione di responsabilità che suggerisce che questo ruolo possa essere detenuto anche dal responsabile della protezione dei dati designato. [29]

Violazione dei dati [modifica]

Ai sensi del GDPR, il responsabile del trattamento dei dati ha l'obbligo giuridico di informare l'autorità di vigilanza senza indebito ritardo, a meno che la violazione non risulti in un rischio per i diritti e le libertà delle persone. Le segnalazioni di violazione dei dati per la segnalazione (articolo 33) sono trascorse al massimo 72 ore. Gli individui devono essere informati se viene determinato un impatto negativo (articolo 34). Inoltre, il responsabile del trattamento dei dati dovrà notificare il responsabile del trattamento senza indebiti ritardi dopo aver preso conoscenza di una violazione dei dati personali (articolo 33).

Tuttavia, l'informativa agli interessati non è richiesta se il responsabile del trattamento dei dati ha attuato misure tecniche e organizzative di protezione adeguate che rendono i dati personali incomprensibili a qualsiasi persona che non è autorizzata ad accedervi, come la crittografia (articolo 34).

Sanzioni [modifica]

Le seguenti sanzioni possono essere imposte:

- un avvertimento scritto in caso di non conformità prima e non intenzionale
- regolari controlli periodici di protezione dei dati
- una multa fino a 10 milioni di euro o fino al 2% del fatturato annuo mondiale dell'esercizio precedente nel caso di un'impresa, a seconda di quale sia maggiore, se vi è stata una violazione delle seguenti disposizioni: (articolo 83, paragrafo 5 e 6 [30])
    - gli obblighi del responsabile del trattamento e dell'incaricato del trattamento ai sensi degli articoli 8, 11, 25-39, 42 e 43
    - gli obblighi dell'organismo di certificazione di cui agli articoli 42 e 43

    - gli obblighi dell'organismo di controllo ai sensi dell'articolo 41, paragrafo 4
- una multa fino a 20 milioni di euro o fino al 4% del fatturato annuo mondiale dell'esercizio precedente nel caso di un'impresa, a seconda di quale sia maggiore, se vi è stata una violazione delle seguenti disposizioni: (Articolo 83, paragrafo 4 [30])
    - i principi di base per il trattamento, comprese le condizioni per il consenso, ai sensi degli articoli 5, 6, 7 e 9
    - i diritti degli interessati ai sensi degli articoli da 12 a 22
    - i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale ai sensi degli articoli da 44 a 49
    - eventuali obblighi ai sensi della legislazione degli Stati membri adottata ai sensi del capitolo IX
    - inosservanza di un ordine o di una limitazione temporanea o definitiva del trattamento o della sospensione dei flussi di dati da parte dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2 o del mancato accesso in violazione dell'articolo 58, paragrafo 1

Marketing B2B [modifica]

All'interno del GDPR c'è una netta differenza tra il business to consumer (B2C) e il business to business (B2B). Secondo il GDPR, ci sono sei motivi altrettanto validi per elaborare i dati personali. Ci sono due di questi che sono rilevanti per dirigere il marketing B2B, sono il *consenso* o l' *interesse legittimo* . Il considerando 47 del GDPR afferma che "il trattamento di dati personali a fini di marketing diretto può essere considerato effettuato per un interesse legittimo". [31]

L'utilizzo *dell'interesse legittimo* come base per il marketing B2B implica che vengano soddisfatte le condizioni chiave:

- "Il trattamento deve riguardare gli interessi legittimi della vostra azienda o di una terza parte specificata, a condizione che gli interessi oi diritti fondamentali dell'interessato non prevalgano sull'interesse legittimo dell'azienda".
- "Il trattamento deve essere necessario per raggiungere gli interessi legittimi dell'organizzazione". [32]

Inoltre, l'articolo 6.1 (f) del GDPR stabilisce che il trattamento è lecito se è "Necessario ai fini degli interessi legittimi perseguiti dal responsabile del trattamento o da una terza parte, eccetto laddove tali interessi siano ignorati dagli interessi o dalle i diritti e le libertà dell'individuo che richiedono la protezione delle informazioni personali, in particolare quando l'individuo è un bambino ". [32]

Pertanto, le aziende possono continuare a utilizzare i dati di marketing ai fini dell'impegno B2B purché siano adottate le misure appropriate per garantire che i dati siano allineati a un obiettivo o campagna specifico. Una frase che viene ora utilizzata è "Marketing corretto per la persona corretta". Come parte di queste società sarà necessario mantenere aggiornati i database di marketing e il CRM al fine di eseguire controlli legittimi sul saldo legittimo. [33]

La Commissione Europea ha affermato che " le leggi sulla privacy dei dati unificate creeranno opportunità straordinarie e motivanti l'innovazione per le imprese non solo in Europa ma anche per l'organizzazione che è disposta a fare affari con gli stati europei o già a gestire gli affari negli stati europei". La commissione si propone che le aziende mantengano le comunicazioni e costruiscano una regolamentazione che sostenga le relazioni reciproche per garantire le migliori pratiche sui dati attraverso *legittimi controlli di equilibrio* [33]

Restrizioni [modifica]

I seguenti casi non sono coperti dal regolamento:

- Intercettazione legale, sicurezza nazionale, militare, polizia, giustizia
- Analisi statistica e scientifica
- Le persone decedute sono soggette alla legislazione nazionale
- Esiste una legge dedicata sulle relazioni tra datore di lavoro e dipendente
- Trattamento di dati personali da parte di una persona fisica nel corso di un'attività puramente personale o domestica

Viceversa, un'entità o più precisamente una "impresa" deve essere impegnata in "attività economica" che deve essere coperta dal GDPR. [a] L'attività economica è definita in ampia misura dal diritto della concorrenza dell'Unione europea . [34]

Ricezione [modifica]

La proposta per il nuovo regolamento ha suscitato molte discussioni e polemiche. [35] [36] Sono stati proposti migliaia di emendamenti. [37]

L'area del consenso del GDPR ha una serie di implicazioni per le aziende che registrano le chiamate come una questione di pratica. Un tipico disclaimer non è considerato sufficiente per ottenere il presunto consenso a registrare le chiamate. Inoltre, quando la registrazione è iniziata, se il chiamante ritira il proprio consenso, l'agente che riceve la chiamata deve essere in grado di interrompere una registrazione avviata in precedenza e assicurarsi che la registrazione non venga memorizzata. [38]

I professionisti IT si aspettano che la conformità con il GDPR richiederà ulteriori investimenti complessivi: oltre l'80% degli intervistati prevede una spesa relativa al GDPR di almeno $ 100.000 USD. [39] Le preoccupazioni sono state riprese in un rapporto commissionato dallo studio legale Baker & McKenzie che ha rilevato che "circa il 70% degli intervistati ritiene che le organizzazioni dovranno investire budget / sforzi aggiuntivi per rispettare il consenso, la mappatura dei dati e il cross-border requisiti per il trasferimento dei dati ai sensi del GDPR. " [40] Il costo totale per le imprese dell'UE è stimato in circa € 200 miliardi, mentre per le società statunitensi la stima è di $ 41,7 miliardi. [41] È stato sostenuto che le piccole imprese e le società di avviopotrebbe non avere le risorse finanziarie per adeguarsi adeguatamente al GDPR, a differenza delle più grandi aziende tecnologiche internazionali (come Facebook e Google) che il regolamento è apparentemente destinato a colpire in primo luogo e in primo luogo. [42] [43] Una mancanza di conoscenza e comprensione dei regolamenti è stata anche una preoccupazione per la sua adozione. [44] Una contro-argomentazione è stata che le società sono state messe al corrente di questi cambiamenti due anni prima che entrassero in vigore e, pertanto, avrebbero avuto tempo sufficiente per prepararsi. [45]

I regolamenti, incluso se un'azienda deve avere un responsabile della protezione dei dati, sono stati criticati per il potenziale onere amministrativo e per i requisiti di conformità non chiari. [46] Sebbene la minimizzazione dei dati sia un requisito, con la pseudonimizzazione come uno dei possibili mezzi, il regolamento non fornisce indicazioni su come o cosa costituisce un efficace sistema di de-identificazione dei dati, con un'area grigia su ciò che sarebbe considerato come inadeguato soggetto di pseudonimizzazione alla Sezione 5 azioni di applicazione. [47] [48] [49] C'è anche preoccupazione riguardo all'implementazione del GDPR in sistemi blockchain , poiché la registrazione trasparente e fissa delle transazioni di blockchain contraddice la natura stessa del GDPR.[50] Molti media hanno commentato l'introduzione di un " diritto alla spiegazione " delle decisioni algoritmiche, [51] [52]ma gli studiosi legali hanno da allora sostenuto che l'esistenza di tale diritto è altamente poco chiara senza test giudiziari ed è limitata nel migliore dei casi [53] [54]

Il GDPR ha raccolto il sostegno delle aziende che lo considerano un'opportunità per migliorare la gestione dei dati. [55] [56] Mark Zuckerberg lo ha anche definito un "passo molto positivo per Internet". [57] I gruppi per i diritti dei consumatori come The European Consumer Organisation sono tra i sostenitori più vocali della legislazione. [58] Altri sostenitori hanno attribuito il suo passaggio al informatore Edward Snowden . [59] Il sostenitore del software libero Richard Stallman ha elogiato alcuni aspetti del GDPR ma ha chiesto ulteriori misure di salvaguardia per impedire alle aziende tecnologiche di "consenso alla produzione". [60]

Impatto [modifica]

Il passaggio alla data di efficacia del GDPR ha portato molte aziende e siti Web a modificare le proprie politiche sulla privacy e le funzionalità in tutto il mondo al fine di soddisfare i propri requisiti, fornendo e-mail e notifica in loco delle modifiche, nonostante avesse avuto almeno due anni per prepararsi e farlo. Questo è stato criticato per aver portato alla fine a una forma di fatica tra gli utenti finali rispetto al numero eccessivo di messaggi. Gli esperti hanno anche notato che alcune e-mail di promemoria affermavano erroneamente che era necessario ottenere un nuovo consenso per l'elaborazione dei dati per il GDPR, anche se il consenso all'elaborazione precedentemente ottenuto è valido purché sia adeguatamente documentato e soddisfi i requisiti del GDPR (considerando 171). Phishingle truffe sono emerse anche utilizzando versioni contraffatte di tali e-mail e si è

anche sostenuto che alcune e-mail di avviso GDPR potrebbero essere state effettivamente inviate in violazione delle leggi anti-spam. [61] [12] L' adozione in massa degli standard di privacy GDPR da parte di società internazionali è stata citata come un esempio dell'effetto " Bruxelles ", un fenomeno in cui le leggi e le normative europee sono utilizzate come riferimento globale a causa della loro gravità. [62]

La ricerca indica che circa il 25% delle vulnerabilità del software ha implicazioni GDPR. [63] Poiché l'articolo 33 sottolinea le violazioni, non i bug, gli esperti di sicurezza consigliano alle società di investire in processi e capacità per identificare le vulnerabilità prima che possano essere sfruttate, compresi i processi di divulgazione delle vulnerabilità coordinate . [64] [65]

Il diluvio di comunicazioni relative al GDPR ha ispirato anche meme , compresi quelli relativi alle comunicazioni sulla privacy che sono state fornite con mezzi atipici (come una tavola Ouija e una striscia di apertura di *Star Wars*), suggerendo che la lista "cattiva o simpatica" di Babbo Natale ha violato il GDPR, e una registrazione di estratti dal regolamento di un ex annunciatore della BBC Radio 4 , nello stile delle sue Previsioni di spedizione a tarda notte . Un blog, *GDPR Hall of Shame*, è stato anche creato per mostrare inusuali comunicazioni GDPR e tentativi di conformità che contenevano gravi violazioni dei requisiti del regolamento. Il suo autore ha osservato che il regolamento "ha molti dettagli non trattati, ma molte informazioni su come rispettare", ma ha anche riconosciuto che le imprese hanno due anni per conformarsi, rendendo ingiustificate alcune delle sue risposte. . [66] [67] [68] [69] [70]

Alla data effettiva, alcuni siti Web internazionali hanno iniziato a bloccare interamente gli utenti dell'UE (compresi Instapaper , [71] Unroll.me, [72] e i giornali di proprietà di Tronc , come il *Chicago Tribune* e il *Los Angeles Times*) o reindirizzarli a spogliati versioni dei loro servizi (nel caso di National Public Radio e *USA Today*) con funzionalità limitate e / o nessuna pubblicità, al fine di rimuovere le loro responsabilità. [73] [74] [75] [76] Alcune società, come Kloute diversi videogiochi online hanno cessato completamente le operazioni in coincidenza con la sua implementazione, citando il GDPR come un onere per le loro operazioni continue, soprattutto a causa del modello di business del primo. [77] [78] [79] Il volume delle vendite di annunci pubblicitari comportamentali online in Europa è diminuito del 25-40% il 25 maggio 2018. [80]

Facebook e sussidiarie WhatsApp e Instagram , così come Google LLC (con targeting per Android), sono stati immediatamente denunciati dal NoYB no profit di Max Schremspoche ore dopo la mezzanotte del 25 maggio 2018, per il loro uso del "consenso forzato". Schrems afferma che entrambe le società hanno violato l'articolo 7, paragrafo 4, non presentando opt-in per il consenso al trattamento dei dati su base individuale e richiedendo agli utenti il consenso a tutte le attività di trattamento dei dati (comprese quelle non strettamente necessarie) o l'utilizzo dei servizi . [81] [82] [83] [84] [85]

Dopo l'implementazione del GDPR, lo stato della California negli Stati Uniti ha approvato una legge simile denominata The California Consumer Privacy Act del 2018.