cedam.it
software and management

INGEGNERIA GESTIONALE

40 anni di attività
1978-2018

GDPR 2018

Questa Mini-Guida intende offrire un panorama delle principali problematiche che le Imprese e soggetti pubblici dovranno tenere presenti in vista della piena applicazione del regolamento, prevista il 25 maggio 2018.

SOMMARIO

Che cos'è il GDPR?

General **D**ata **P**rotection **R**egulation.

Un regolamento europeo sulla protezione dei dati personali che, a partire dal 25 MAGGIO 2018, sostituisce le leggi esistenti sulla protezione dei dati in tutti gli Stati membri dell'UE.

Lo scopo del regolamento è di proteggere i dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale, dall'alterazione, dall'accesso o divulgazione non autorizzati, e da qualsiasi altra forma illecita di trattamento.

GDPR sarà applicato inderogabilmente dal 25 MAGGIO 2018.

La decisione del Regno Unito di lasciare l'UE non ne influenzerà l'entrata in vigore.

A chi si applica il regolamento GDPR?

Il GDPR vale per i soggetti e le organizzazioni che trattano dati personali all'interno dell'UE o trattano dati fuori dall'UE, ma che fanno riferimento a cittadini europei.

I *titolari del trattamento* dei dati personali sono persone fisiche o "persone giuridiche", e sono coloro che determineranno le finalità, le condizioni e gli strumenti per il trattamento dei dati personali.

Titolare potrebbe essere ad esempio un medico con i dati dei pazienti.

I *responsabili del trattamento* sono le entità che elaborano i dati per conto dei titolari del trattamento.

Ad esempio un'organizzazione che memorizzi, digitalizzi e cataloghi tutte le informazioni prodotte su carta da parte di una banca.

A quali dati si applica il GDPR?

Il GDPR si applica ai dati personali.

I *dati personali* sono informazioni che possono essere utilizzate, da sole o con altre informazioni, per identificare l'utente come persona.

Ad esempio:

Nome	*Codice Fiscale*
Cognome	*Numero di Passaporto*
Data di Nascita	*Indirizzi IP (associato ad altre informazioni)*
Indirizzo di Casa	*Targa Automobilistica*
Indirizzo email	*Patente di Guida*
Numero di Telefono	*Dati Biometrici o Calligrafici*
Documentazione Sanitaria	*Informazione Genetica*

Come fanno le organizzazioni a raggiungere la conformità sul GDPR?

Esse **devono elaborare tutti i dati personali in modo lecito, con correttezza e in modo trasparente**.

I dati personali devono essere rilevati solo per finalità determinate, esplicite e legittime.

I dati personali devono essere elaborati in modo da garantire l'adeguata sicurezza degli stessi.

"*Privacy by design*": il tema della privacy by design permea il GDPR, con l'obiettivo che la sicurezza sia considerata come parte fondamentale già in fase di progetto e di utilizzo di tutti quei prodotti o servizi che gestiscano dati personali.

Le aziende dovranno implementare la privacy fin dall'inizio di qualsiasi progetto che coinvolga informazioni personali.

Responsabili della protezione dei dati (DPO) sono necessari quando:

- Il trattamento dei dati personali è ad opera di autorità pubbliche.

- L'elaborazione viene eseguita dai soggetti che regolarmente e sistematicamente trattano dati personali su larga scala.

- Il soggetto tratta su larga scala categorie specifiche di dati '*speciali',* ad esempio idonei a rivelare:

• salute

• origine razziale o etnica

• opinioni politiche

• convinzioni religiose o filosofiche

• appartenenza a sindacati

• condanne penali

Si noti che anche se una prima bozza della GDPR limitava l'obbligatorietà del DPO alle aziende con più di 250 dipendenti o che trattano dati personali per 5.000 o più soggetti, la versione finale non ha alcuna restrizione in merito.

Le organizzazioni dovranno quindi considerare:

Di quali dati personali sono titolari.
Dove i dati personali vengono memorizzati.
Come i dati personali vengono memorizzati.
Chi può accedere ai dati personali.
Come si ottiene l'accesso ai dati personali.
Chi sta monitorando i dati personali.
Come i dati personali sono accessibili su richiesta.
Come i dati personali possono essere cancellati su richiesta.

GDPR Data Breach

Il GDPR definisce la violazione dei dati come una violazione della sicurezza che conduce ad accesso, distruzione, perdita, alterazione o divulgazione non autorizzata dei dati personali.

Questo significa che una violazione dei dati è molto più della sola perdita dei dati personali.

Ad esempio:

- Un ospedale potrebbe essere responsabile di una violazione se la cartella clinica di un paziente risultasse accessibile in modo inappropriato a causa di una mancanza di adeguati controlli interni.

- Una banca potrebbe essere responsabile di una violazione se i dati personali dei loro clienti venissero distrutti a causa di un'infezione da "ransomware".

Una violazione dei dati potrebbe essere causata dall'interno.

Ad esempio:

- Perdita accidentale dei dati personali, ad esempio attraverso lo smarrimento di un laptop o di un dispositivo mobile non crittografati.

- Divulgazione accidentale dei dati personali, ad esempio l'invio di una email contenente dati personali non crittografati al di fuori dell'organizzazione.

- Furto deliberato dei dati personali, ad esempio l'esportazione con dispositivi di archiviazione USB.

Una violazione dei dati potrebbe essere causata dall'esterno.

Ad esempio:

- Attacco mirato ai sistemi che contengono dati personali.

- Perdita dei dati portata dall'infezione dei sistemi da parte di un "malware".

GDPR Notifica Violazione dei Dati

I titolari del trattamento sono tenuti a segnalare una violazione dei dati all'autorità di vigilanza competente senza indebito ritardo.

• Nel caso in cui la violazione dei dati personali possa provocare un rischio elevato ai diritti e le libertà di un soggetto, il titolare del trattamento deve comunicare la violazione all'interessato senza indebito ritardo.

• Nel caso in cui la violazione non arrechi un rischio per i diritti e le libertà delle persone interessate, andrà comunicata entro e non oltre le 72 ore successive alla scoperta.

FONDAMENTI DI LICEITA' (Legittimità) DEL TRATTAMENTO

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice** (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

In particolare:

- **Per i dati "sensibili" (si veda art. 9 regolamento) il consenso** DEVE **essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione — art. 22).**
- NON **deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1)** DEVE **essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.**

INFORMATIVA

Contenuti dell'informativa:

I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare DEVE SEMPRE specificare i dati di contatto del RPD-DPO, ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.). Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di

conservazione, e il diritto di presentare un reclamo all'autorità di controllo. Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa:

Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa:

Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee *(si veda anche considerando 58)*. L'informativa è data, **in linea di principio, per iscritto** e **preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: *si vedano art. 12, paragrafo 1, e considerando 58*), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra *(art. 12, paragrafo 1)*. Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** *(art. 12, paragrafo 7)*; queste icone dovranno essere identiche in tutta l'UE e saranno definite prossimamente dalla Commissione europea. Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** *(si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo)*, anche se occorre sottolineare che **spetta al titolare**, in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** *(si veda art. 14, paragrafo 5, lettera b)* — a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

L'informativa *(disciplinata nello specifico dagli artt. 13 e 14 del regolamento)* deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato — art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano**, le **finalità del trattamento**, i **diritti degli interessati** (compreso il

diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

DIRITTI DEGLI INTERESSATI

Il termine per la risposta all'interessato, per tutti i diritti (compreso il diritto di accesso) è di **1 mese**, estendibili fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.**

Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive** (anche ripetitive)*(art. 12.5)*, a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso *(art. 15, paragrafo 3)*; in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato **oralmente solo se così richiede l'interessato** stesso *(art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3)*.

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.

Diritto di Accesso (art. 15):

Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento.

Fra le informazioni che il titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

Diritto di cancellazione (diritto all'oblio) (art.17):

Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) **di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati,** compresi "qualsiasi link, copia o riproduzione" *(si veda art. 17, paragrafo 2)*.

Ha **un campo di applicazione più esteso** di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento *(si veda art. 17, paragrafo 1)*.

TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO

Il regolamento:

- disciplina la **contitolarità del trattamento** *(art. 26)* e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- fissa più dettagliatamente *(rispetto all'art. 29 del Codice)* le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" — quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, le categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

- consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile *(si veda art. 28, paragrafo 4)*, per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" *(si veda art. 82, paragrafo 1 e paragrafo 3)*;

- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti *(ex art. 30, paragrafo 2)*; l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti *(ex art. 32 regolamento)*; la **designazione di un RPD-DPO**, nei

casi previsti dal regolamento o dal diritto nazionale *(si veda art. 37 del regolamento)*. Si ricorda, inoltre, che **anche il responsabile** non stabilito nell'UE dovrà **designare un rappresentante** in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento — diversamente da quanto prevede oggi l'art. 5, comma 2, del Codice.

APPROCCIO BASATO SUL RISCHIO E MISURE DI ACCOUNTABILITY (RESPONSABILIZZAZIONE) DI TITOLARI E RESPONSABILI

- Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili — ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento *(si vedano artt. 23–25, in particolare, e l'intero Capo IV del regolamento)*. Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali — nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

- Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" *(si veda art. 25)*, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati — tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

- Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il rischio inerente al trattamento. Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati *(si vedano considerando 75–77)*; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione *(si vedano artt. 35–36)* tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il

trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

- Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto *prior checking* (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia. Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.
- Queste le principali novità in termini di adempimenti da parte di titolari e responsabili del trattamento.

Registro dei trattamenti:

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio *(si veda art. 30, paragrafo 5)*, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico — **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche — ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti. Nello specifico, si richiama l'attenzione sulla sostanziale **coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice e quelli che devono costituire il registro dei trattamenti ex art. 30 regolament**o;

l'Autorità sta valutando di mettere a disposizione un modello di registro dei trattamenti sul proprio sito, che i singoli titolari potranno integrare nei modi opportuni.

Misure di sicurezza:

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva** ("tra le altre, se del caso"). Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** *(ex art. 33 Codice)* poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Nuove sanzioni previste

Il primo dato chiave del nuovo regolamento è che sono previste sanzioni elevate in caso di violazioni. Le categorie di sanzioni sono due:

Categoria 1 - Fino a EUR 10 milioni o fino al 2% del fatturato mondiale totale annuo, se superiore.

Questa categoria di sanzione verrà applicata in caso di violazioni delle disposizioni dove, per esempio, non vi è alcun contratto scritto tra il titolare del trattamento e il responsabile del trattamento. È ora responsabilità delle organizzazioni in possesso dei dati personali e sensibili di un soggetto e titolari del trattamento accertarsi che sia in vigore un contratto scritto sintetico nel caso di cessione a un terzo (responsabile del trattamento).

Non hai un contratto? In arrivo una sanzione.

Categoria 2 - Fino a EUR 20 milioni o fino al 4% del fatturato mondiale totale annuo, se superiore.

Questa categoria si applica per esempio laddove un'impresa non ottenga l'esplicito consenso da parte di un interessato per il trattamento di dati personali sensibili.