REGOLAMENTO UE 2016/679

Ad un anno dall'entrata in vigore

L'importanza dell' ACCOUNTABILITY nelle sanzioni

09 ottobre 2019 Alessandra Andrioli – Consulente Direzionale
SENIOR CONSULTANT PROFILI & CARRIERE
Data Protection Officer

LE FINALITA' REG. UE 679/2016

1. UNIFORMA LE MODALITA' DI TRATTAMENTO DEI DATI PERSONALI

   ENTRO I CONFINI UE;

2. ACCRESCERE IL DIRITTO PER GLI INDIVIDUI ;

2. RAFFORZA GLI OBBLIGHI IN CAPO ALLE AZIENDE;

3. UNIFORMA IL QUADRO SANZIONATORIO :

   → PER ENTITA' ;

   → PER IPOTESI PER CUI POSSONO ESSERE COMBINATE

SINTESI

- APPROVATO : APRILE 2016
- E' ENTRATO IN VIGORE : 25 MAGGIO 2018
- ELENCO DEI DIRITTI DEI LAVORATORI:

→ art. 15 – diritto di accesso;

→ art. 16 – diritto di rettifica;

→ art. 17 – diritto alla cancellazione / diritto all'oblio;

→ art.18 - diritto alla limitazione di trattamento;

→ art.19 - obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento;

→ art. 20-diritto alla portabilità dei dati;

→ art. 21- diritto di opposizione;

→ art. 22 - profilazione

- NOVITA' 679/2016 : POLICY

  - **PRINCIPIO BY DESIGN / BY DEFAULT**;

  - **DPO** (deve vigilare sull'applicazione della regolamento oltre ad essere elemento di contatto con le autorità di controllo) ;

  - **VALUTAZIONE D'IMPATTO** (ANALISI DEL RISCHIO – DATA BREACK);

  - **ACCOUNTABILITY** (ART. 5) - REGISTRO DELLE ATTIVITA' DI TRATTAMENTO;

  - INTRODUZIONE DI NUOVI CONCETTI:

    → MINIMIZZAZIONE DEI DATI;

    → RESPONSABILITA' ;

    → VERIFICABILITA' ;

    → TEMPESTIVITA';

    → CONFORMITA' ;

    → AUDIT INTENI ED ESTERNI;

    → MISURE DI SICUREZZA : ADEGUATE D EFFICACI;

La Privacy in azienda in sintesi

- 1. SINTESI SCHEMATICA DEL QUADRO NORMATIVO DA ESPORRE : PRIVACY;
- 2. ORGANIGRAMMA PRIVACY e POLICY ACCOUNTABILITY:

  RUOLI E RESPONSABILITA';
- 3. PROTEZIONE DEI DATI e TUTELA DELLA PRIVACY DEI LAVORATORI;
- 4. VALUTAZIONE D'IMPATTO PER LA PROTEZIONE DEI DATI (DPIA) ;
- 5. ESERCIZIO DEI DIRITTI DELL'INTERESSATO (lavoratore) e AZIONI LEGALI;
- 6. IL RECLAMO, DATA BREACK;
- 7. INCARICO AL RESPONSABILE, al DPO ;
- 8. INFORMATIVA AI DIPENDENTI;
- 9. SEGNALAZIONE VIDEO SORVEGLIANZA .

I cardini delle Regolamento 679/2016

- Questo nuovo sistema si basa su alcuni principi cardini ineludibili.

  I primi tre sono :

- La necessità di un'analisi del rischio;
- La stretta connessione con la migliore tecnica e i costi da supportare;
- La comprenzione e l'applicazione COSTANTE della nozione di ACCOUNTABILITY.

Accountability

- Stabilisce la responsabilità generale del titolare e/o responsabile del trattamento *per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto*.

  In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto *misure ADEGUATE* **ed** *EFFICACI ed essere* **in grado di DIMOSTRARE la CONFORMITA' delle attività di trattamento con il presente regolamento, COMPRESA L'EFFICACIA DELLE MISURE.** Tali misure dovrebbero **tenere conto: della → NATURA; → dell'AMBITO DI APPLICAZIONE; → del CONTESTO; → delle FINALITA'DEL TRATTAMENTO; → del RISCHIO (diretto e indiretto) per i diritti e le libertà delle persone fisiche**

Principio della accountability

- Tutto il sistema deve essere visto sotto due aspetti, al fine di rispettare anche il principio della accountability:

  → gli adempimenti devono essere *concretamente svolti ("sostanza");*

  → tutto ciò che viene fatto deve essere anche *formalmente verificabile ("verificabilità")*, sia dall'interno, sia da eventuali operazioni di auditing esterno.

  *Ciò comporta la necessità di **tenere traccia** di qualsiasi operazione effettuata in un'ottica di protezione dei dati, al fine di poter ripercorrere in modo obiettivo, in ogni momento, il percorso seguito e valutare i risultati.*

Gli elementi dell'accountabiliy

- La TRASPARENZA intesa come garanzia della compelta *accessibilità* alle informazioni, per i dipendenti, cittadini e utenti;

- La RESPONSIVITA' intesa come *capacità di rendere conto* di scelte, comportamenti e azioni e di rispondere alle questioni poste dagli stakeholde;

- La COMPLIANCE intesa come capacità di far *rispettare le norme*

Art. 5 - accountability

- Liceità, correttezza e trasparenza: trattamento → LECITO, → CORRETTO, → TRASPERENTE ;
- Limitazione delle finalità: i dati devono essere raccolti per *finalità determinante, esplicite e legittime*, *e* successivamente *trattati in modo non incompatibile con tali finalità;*
- Minimizzazione dei dati: devono essere → ADEGUATI, → PERTINENTI, → LIMITATI a quanto necessario;
- Esattezza: → ESATTI e, se necessario, AGGIORNATI; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti;
- Limitazione della conservazione: conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità;
- Integrità e riservatezza: trattati in modo *da garantire* ***un'adeguata sicurezza*** *dei dati personali, compresa la protezione*, mediante misure tecniche e organizzative adeguate, *da trattamenti non autorizzati o illeciti e dalla perdita,* dalla *distruzione* o dal *danno accidentale*;

Sappiamo che la volontà del GDPR è quella di **UNIFORMARE Le modalità di gestione dei dati nonche LA *TIPOLOGIA* E L'*ENTITA'* DELLE SANZIONI**,

Quindi :

→ ***l'applicazione coerente delle norme sulla protezione dei dati personali in un regime di protezione dei dati armonizzato per tutti i cittadini europei.***

→ ***un QUADRO SANZIONATORIO privacy più severo :***

→ ***per l' ENTITA' degli importi;***

→ *per le ipotesi per cui possono essere COMBINATE le sanzioni;*

Sulla base dell'**art. 82 del GDPR**, resta fatta la salva la possibilità per l'interessato, che subisca un danno materiale o immateriale, di ottenere il risarcimento del danno, a seconda che la violazione sia commessa da Titolare o dal Responsabile.

Art.82 : diritti al risarcimento e responsabilità

- Diritto al risarcimento:

  1. Chiunque subisca un DANNO MATERIALE O IMMATERIALE causato da una violazione del regolamento ue 679/2016, HA IL DIRITTO DI OTTENERE IL RISARCIMENTO da parte del Titolare del Trattamento e/o da parte Responsabile del Trattamento

  Responsabilità:

  2. il TITOLARE DEL TRATTAMENTO COINVOLTO nel trattamento RISPONDE per il danno CAGIONATO dal suo trattamento che violi il regolamento 679/2016.

  il RESPONSABILE del Trattamento RISPONDE per il DANNO causato dal trattamento SOLO **SE NON HA** ADEMPIUTO gli OBBLIGHI del regolamento 679/2016 diretti ai responsabili del Trattamento o ha AGITO IN modo DIFFORME o CONTRARIO rispetto alle legittime ISTRUZIONI del titolare del trattamento.

  3. il TITOLARE del trattamento o IL RESPONSABILE del trattamento E' ESONERATO DALLA RESPONSABILITA' se DIMOSTRA che l'evento dannoso non gli è imputabile in alcun modo

4. Qualora *più* Titolari del trattamento o Responsabili del Trattamento oppure entrambi il Titolare del Trattamento e il Responsabile del trattamento SIANO COINVOLTI nello stesso trattamento e siano RESPONSABILI dell'eventuale danno causato dal Trattamento , OGNI TITOLARE del Trattamento o RESPONSABILE del trattamento E' RESPONSABILE IN SOLIDO PER L'INTERO AMMONTARE DEL DANNO, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un Titolare del trattamento o un Responsabile del trattamento ABBIA PAGATO L'INTERO RISARCIMENTO DEL DANNO, tale titolare del trattamento o Responsabile del trattamento HA IL DIRITTO DI RECLAMARE DAGLI ALTRI Titolari del Trattamento o Responsabile del Trattamento COINVOLTI nello stesso trattamento LA PARTE DEL RISARCIMENTO CORRISPONDENTE ALLA LORO PARTE DI RESPONSABILITA' .

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno verranno promosse dinnanzi alle autorità giurisdizionali competenti

POTERI DELLE AUTORITA' DI CONTROLLO

→ POTERI DI INDAGINE;

→ POTERI CORRETTIVI;

→ POTERI AUTORIZZATIVI E CONSULTIVI.

- *Eventuali altri poteri che possono essere attribuiti dalle autorità degli stati membri*

ART. 58 POTERI

- 1. Ogni autorità di controllo ha tutti i seguenti POTERI DI INDAGINE:

  → INGIUNGERE al titolare del trattamento e al Responsabile del Trattamento e, ove applicabile, al rappresentante del trattamento o del responsabile del trattamento, DI FORNIRE ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;

  → CONDURRE INDAGINI sotto forma di REVISIONE sulla protezione dei dati;

  → EFFETTUARE un RIESAME delle certificazioni rilasciate in conformità dell'art. 42, paragrafo 7, (regolamento ue 679/2016);

  → NOTIFICARE al titolare del trattamento o al Responsabile del trattamento *le presunte* violazioni del regolamento ue 679/2016 ;

  → OTTENERE, dal titolare del trattamento o dal responsabile del trattamento, L'ACCESSO A TUTTI I DATI PERSONALI e a tutte LE INFORMAZIONI necessarie per l'esecuzione dei suoi compiti;

  → OTTENERE L'ACCESSO a TUTTI I LOCALI del titolare del trattamento e del responsabile del trattamento, compresi GLI STRUMENTI E MEZZI del trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

- 2. Ogni autorità di controllo ha tutti i seguenti POTERI CORRETTIVI:

  → Rivolgere AVVERTIMENTI al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti POSSONO VEROSIMILMENTE VIOLARE le disposizioni del regolamento ue 679/2016

  → rivolgere AMMONIMENTI al titolare del trattamento o al responsabile del trattamento OVE I TRATTAMENTI abbiano VIOLATO le disposizioni del reg. ue 679/2016

  → INGIUNGERE al titolare del trattamento o al responsabile del trattamento DI SODDISFARE LE RICHIESTE dell'interessato di esercitare i diritti loro derivanti dal reg. ue 679/2016

  → INGIUNGERE al titolare o al responsabile del trattamento DI CONFORMARE i trattamenti ALLE DISPOSIZIONI del reg. ue 679/2016, se del caso, *in un determinato modo ed entro un determinato termine*

  → INGIUNGERE al titolare del trattamento di COMUNICARE all'interessato una VIOLAZIONE dei dati personali;

  → IMPORRE una LIMITAZIONE PROVVISORIA o DEFINITIVA al trattamento, incluso il DIVIETO DI TRATTAMENTO

→ ORDINARE la RETTIFICA, LA CANCELLAZIONE di dati personali o la LIMITAZIONE del trattamento a norma degli art. 16,17,e 18 e la NOTIFICAZIONE *di tale misura ai destinatari cui sono stati comunicati i dati personali* ai sensi dell'art. 17 paragrafo 2 e art. 19;

→ REVOCARE LA CERTIFICAZIONE o INGIUNGERE all'organismo di certificazione di RITIRARE la certificazione rilasciata a norma degli art. 42 e 43, oppure INGIUNGERE ALL'ORGANISMO di certificazione di NON RILASCIARE LA CERTIFICAZIONE SE I REQUISITI per la certificazione NON SONO PIU' SODDISFATTI;

→ INGIUNGERE una sanzione amministrativa pecuniaria ai sensi dell'art.83, *in aggiunta alle misure in elenco,*o in luogo di tale misure, in funzione delle circostanze di ogni singolo caso;

→ ORDINARE LA SOSPENSIONE dei flussi di dati verso un destinatario in un *paese terzo o un'organizzazione internazionale.*

- 3. Ogni autorità di controllo ha tutti seguenti i POTERI AUTORIZZATIVI E CONSULTIVI :

  → FORNIRE CONSULENZA al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'art. 36;

  → RILASCIARE, di propria iniziativa o su richiesta, PARERI d*estinati al parlamento* nazionale, al governo dello stato membro, oppure, conformemente al diritto degli stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;

  → AUTORIZZARE il trattamento di cui all'art. 36 paragrafo 5, se il diritto dello stato membro richiede una siffatta autorizzazione preliminare;

  → RILASCIARE *parere su progetti di codici di condotta e approvarli*, ai sensi dell'art.40 paragrafo 5;

  → ACCREDITARE *gli organismi di certificazione* a norma dell'art. 43;

  → RILASCIARE *certificazioni e approvare i criteri di certificazione* conformemente all'art. 42 paragrafo 5;

  → ADOTTARE *le clausole di protezione dei dati* di cui all'art. 28 paragrafo 8 e all'art. 46 paragrafo 2 lettera d;

  → AUTORIZZARE *le clausole contrattuali* di cui all'art. 46 paragrafo 3 lettera a;

→ AUTORIZZARE gli accordi amministrativi di cui all'art. 46 paragrafo 3 lettera b;

→ APPROVARE le norme vincolanti d'impresa ai sensi dell'art. 4.

- 4. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, *incluso il ricorso* giurisdizionale effettivo *e il giusto processo*, previste dal diritto dell'unione e degli stati membri conformemente alla carta

  5. ogni stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale *in caso di violazione del regolamento 679/2016 per far rispettare le disposizioni dello stesso*

  6. Ogni stato membro *può prevedere per legge che la sua autorità di controllo abbia ulteriori poteri rispetto a quelli di cui ai paragrafi 1,2 e 3 .* L'esercizio di tali poteri non pregiudica l'operatività effettiva del capo VII

§§§§

Le sanzioni

→ Amministrative pecuniarie (considerando 148);

→ Penali;

→ Correttive;

→ Integrative.

Devono essere: → EFFETTIVE - ADEGUATE;

→ EQUILIBRATE;

→ PONDERATE;

→ PROPORZIONATE ;

→ DISSUASIVE

GDPR : ART. 83 LE SANZIONI AMMINISTRATIVE PECUNIARIE E/O PENALI

- Il GDPR, all'art.83 , disciplina le ipotesi per cui è prevista l'applicazione di sanzioni amministrative pecuniarie e/o penali.

- Per quanto riguarda le PRIME (SANZIONI AMMINISTRATIVE PECUNIARIE) esse possono raggiungere i ***10 milioni di euro, se superiore, il 2%*** del fatturato mondiale nei casi di :

  a. VIOLAZIONE delle condizioni applicabili *al consenso dei minori* in relazione ai servizi della società dell'informazione;

  b. trattamento ILLECITO di dati personali c*he non richiede l'identificazione* dell'interessato;

  c. MANCATA o ERRATA notificazione e/o comunicazione di un data breach all'autorità nazionale competente;

  d. VIOLAZIONE dell'obbligo di nomina del DPO;

  e. MANCATA applicazione di misure di sicurezza.

- L'importo delle sanzioni amministrative pecuniarie può salire fino *a **20 milioni di euro**,* o alternativamente, sino *al **4%*** del fatturato mondiale dell'impresa nei casi di :

  a. INOSSERVANZA di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;

  b. TRASFERIMENTO ILLECITO cross-border di dati personali ad un destinatario in un Paese terzo.

- Nonostante il GDPR focalizzi la propria attenzione, prevalentemente, sulle violazioni di tipo amministrativo, all'interno del Considerando **149** è stabilito che gli Stati membri " dovrebbero poter stabilire disposizioni relative a SANZIONI PENAI come strumento di attuazione e tutela della nuova disciplina, pur sempre in ossequio al principio del ne bis in idem.

- All'interno del GDPR è presente anche un *MARGINE DI DISCREZIONALITA'* circa la possibilità di infliggere una sanzione e la determinazione dell'importo della stessa. *Ciò non implica un'autonomia gestionale delle sanzioni in capo alle Autorità nazionali competenti, MA FORNISCE , a queste ultime, alcuni*

criteri su come interpretare le singole CIRCOSTANZE del caso.

- Verranno esaminati di seguito alcuni *CRITERI PER LA DETERMINAZIONE* delle sanzioni amministrative pecuniarie, di cui all'articolo 83 paragrafo 2 :

  → la natura, gravità e durata delle violazioni;

  → il carattere doloso o colposo della violazione;

  → Il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi.

- Con riferimento al primo criterio (= natura, gravità e durata), lo stesso regolamento *riconosce l'esistenza di diversi massimali per le sanzioni amministrative pecuniarie, da 10 a 20 milioni di euro.*

- Sarà compito dell'autorità nazionale competente valutare le circostanze di specie, alla luce di tali criteri generali, e poi decidere se procedere con una misura correttiva, più o meno severa, sotto forma di sanzione pecuniaria.

  All'interno del considerando **148**, è offerta all'autorità nazionale l'opportunità di sostituire le sanzioni pecuniarie con un ammonimento, *"in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica"*.

  Anche tale inciso dimostra la tendenza del legislatore europeo di incoraggiare l'utilizzo di sanzioni pecuniarie con un approccio ponderato ed equilibrato.

  → **L'obiettivo ultimo rimane**, infatti, quello di **incentivare le società al rispetto della PRIVACY BY DESIGN e PRIVACY BY DEFAULT**, *affidando lo strumento dell'applicazione di sanzioni pecuniarie cosi elevate, esclusivamente, al fine di reagire in maniera dissuasiva e proporzionata ad eventuali violazioni.*

- Con riferimento al **secondo criterio** (**DOLOSO e COLPOSO**), le valutazioni, circa l'esistenza di dolo o di colpa nella condotta, verranno effettuate sulla base di elementi oggettivi e sarà compito della giurisprudenza emergente definire ex ante “linee di demarcazione più chiare per valutare il carattere doloso di una violazione” il Working Party ha, tuttavia, già provveduto ad esemplificare alcune condotte che potranno integrare il suddetto **carattere doloso** .

- Queste sono riconducibili alle ipotesi di :

  → trattamenti illeciti autorizzati esplicitamente dal senior management, ovvero ignorando i pareri formulati dal DPO;

  → modifica di dati personali, *avente la finalità di fornire un'impressione “fuorviante”* circa il conseguimento degli obiettivi individuati;

  → vendita di dati, in mancanza di verifica e/o ignorando la scelta liberamente esercitata dagli interessati.

Anche all'interno delle presenti linee guida viene, inoltre, precisato che ***la carenza di risorse economiche e materiali non potrà costituire ipotesi di esenzione di responsabilità.***

In funzione del cosiddetto RISK BASED APPROACH, infatti, il titolare dovrà progettare, sin dal principio, il proprio trattamento, stimando l'esistenza di possibili rischi per i diritti e le libertà degli interessati. **Tale valutazione iniziale determinerà l'entità della responsabilità**, in capo al titolare o al suo responsabile, tenendo in considerazione il contesto, le finalità e la natura del trattamento.

- Con riferimento al **terzo criterio** (*cooperazione*), ciò che deve essere posto in risalto sarà il livello e l'entità della cooperazione con le autorità di controllo. Esso potrà costituire un fattore determinante, *nella scelta di applicare o meno una sanzione amministrativa pecuniaria* e, eventualmente, fissarne l'ammontare, *qualora siano state limitate o azzerate le ripercussioni negative sui diritti degli interessati che si sarebbero altrimenti verificate in mancanza di tale collaborazione (la sanzione deve sempre rispettare i criteri e carattere di effettività, proporzionalità e dissuasività.oltre equilibrio coerenza.)*-

SANZIONI PREVISTE DAL REG. UE 679/2016

Di seguito sono riportate tutte le sanzioni (c.d Multe) previste dal REG. UE 679/2016 che ai sensi dell'art. 83 del regolamento stesso devono avere carattere di EFFETTIVITA', PROPORZIONALITA' e DISSUASIVITA'.

Le sanzione amministartiva pecuniarie, riportate su, possono essere INTEGRATIVE, o COMPLETAMENTE SOSTITUTIVE delle sanzioni correttive e si distinguono in sanzioni di carattere economico e sanzioni correttive.

Le decisoni sull'applicazione della sanzione spetta all'autorità di controllo che, nella valutazione, *tiene conto delle circostanze del singolo caso.* Ossia:

→ della NATURA, GRAVITA', e DURATA della violazione;

→ del carattere DOLOSO o COLPOSO della violazione;

→ delle misure ADOTTATE per ATTENUARE il danno subito dagli interessati;

→ delle eventuali precedenti violazioni commesse dal titolare del trattamento;

→ dal grado di COOPERAZIONE con l'autorità di controllo;

→ ulteriori fattori aggravanti

QUANDO SI APPLICANO LE SANZIONI AMMINISTRATIVO PECUNIARIE

- Quando abbiamo un INNOSSERVANZA:

→ DEGLI OBBLIGLI (2%) FINO A 10 MLN: → DEL *TITOLARE;*

→ DEGLI *ORGANISMI DI CERTIFICAZIONE*;
→ DELL'*ORGANISMO DI CONTROLLO*;

→ DEI PRINCIPI (4%) FINO A 20MLN: → *PRINCIPI* ***BASE DEL REGOLAMENTO***;

→ *DIRITTI DEGLI INTERESSATI*;

→ DELLE DISPOSIZIONI SUI TRASFERIMENTI DEI DATI PERSONALI IN PAESI TERZI;

→ DI UN ORDINE, LIMITAZIONE PROVVISORIA o DEFINITIVA;

→ DI UN ORDINE DI SOSPENSIONE DEI FLUSSI DEI DATI DA PARTE DELLE AUTORITA' DI CONTROLLO;

→ DI UN ORDINE CORRETTIVO (4%) FINO A 20 MLN SANCITO DALL'AUTORITA' DI CONTROLLO

→ LA MANCATA TENUTA DEI REGISTRI DELLE ATTIVITA' DI TRATTAMENTO (2%) FINO A 20MLN

Sanzioni correttive

- Le sanzioni correttive sono connessi ai poteri dell'autorità di controllo. Essi **consistono** nel :

  - rivolgere AVVERTIMENTI al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti POSSONO VIOLARE il GDPR;

  - rivolgere AMMONIMENTI al titolare e del trattamento o al responsabile del trattamento ove i trattamenti ABBIANO VIOLATO le disposizioni del GDPR

  - INGIUNGERE al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti;

  - INGIUNGERE al titolare o al responsabile del trattamento di CONFORMARE i trattamenti alle disposizioni del GDPR, anche specificando in che modo ed entro quale termine;

  - INGIUNGERE al titolare del trattamento di comunicare all'interessato una violazione dei dati personali

  - IMPORRE una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento

  - ORDINARE la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali

  - REVOCARE la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli artt 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti

- Infliggere una sanzione amministrativa pecuniaria in aggiunta alle presenti misure (v. sopra)

- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Con la nuova legislazione in materia di protezione dei dati personali **le aziende che gestiscono i dati personali dei propri dipendenti e cittadini europei dovranno** *sottostare a nuovi obblighi e responsabilità*

I*n caso di mancato rispetto di queste norme*, il GDPR- *consente alle autorità di protezione dei dati personali di emettere multe fino a 20 milioni di euro o fino al 4%* del fatturato mondiale annuo di una società. La violazione degli obblighi del titolare del trattamento e del responsabile del trattamento, per la **tenuta dei registri** dai trattamenti dei dati personali, previsto dall'art. 30 comporta sanzioni pecuniarie fino a euro 10.000.000,00 o per le imprese fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Il regolamento è già in vigore per tutti i dettagli e le casistiche previssute per le sanzioni, si rimanda direttamente al regolamento ue 2016/679 art.83.

Art. 83 GDPR – Regolamento generale sulla Protezione dei Dati (Ue 2016/679) condizioni generali per infliggere sanzioni pecuniarie

Premesso che:

- ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte in relazione alle violazioni del presente regolamento siano in ogni singolo caso effettive, proporzionate e dissuasive.

- Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso *si tiene debito conto dei seguenti elementi:*

  - la natura, la gravità e la durata della violazione **tenendo in considerazione:** la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

CONDIZIONI GENERALI PER INFLIGGERE LE SANZIONI PECUNIARIE

Quindi Le circostanze da tenere conto :

→ NATURA → GRAVITA' → DURATA;

→ IL NUMERO DEI LESI LA CATEGORIA DI DATI INTERESSATI DALLA VIOLAZIONE;

→ IL LIVELLO DEL DANNO; → IL CARATTERE DOLOSO O COLPOSO; → LE MISURE DI SICUREZZA ADOTTATE EX ANTE;

→ LA VALUTAZIONE DEL RISCHIO; → IL GRADO DI RESPONSABILITA';

→ IL GRADO DI COOPERAZIONE; → EVENTUALI PRECEDENTI VIOLAZIONI E RISPETTO DEI PROVVEDIMENTI

→ I TERMINI MEDIANTE I QUALI L' AUTORITA' DI CONTROLLO HA APPRESO DELLA VIOLAZIONE; → SE LA VIOLAZIONE E' STATA NOTIFICATA AGLI INTERESSATI;

→ ADESIONE AI CODICI DI CONDOTTA E DI CERTIFICAZIONE;

→ EVENTUALI BENEFICI DALL'EVENTO DANNOSO

Infine se abbiamo più violazioni, l'importo della sanzione amministrativa pecuniaria non supererà l'importo della violazione più grave

Avere IDEE CHIARE…. DA SUBITO

FINE

Alessandra Andrioli

Consulente Direzionale

Senior Consultant Profili & Carriere

Data Protection Officer

340.4161061

studioandrioli@gmail.com

bologna@profiliecarriere.it - www.profiliecarriere.it