



SERVIZIMPRESA s.r.l.

Il Regolamento EU 2016/679: cosa fare per essere preparati

Con il prossimo 25 maggio 2018, le norme previste dal nuovo Regolamento Europeo 2016/679, in vigore già dal giugno 2016, saranno definitivamente applicabili.

Tra le molte novità che il Regolamento apporterà alla gestione del trattamento dei dati assume maggiore evidenza quella che nel testo inglese è definita "accountability" e che nella versione italiana viene presentata come "responsabilizzazione". In altre parole, il Titolare e il Responsabile avranno il compito di decidere autonomamente la modalità, le garanzie e i limiti dei trattamenti, nel rispetto delle disposizioni normative, assumendo su di sé, la responsabilità per le misure di sicurezza decise ed adottate, al fine di mitigare i rischi connessi al trattamento.

Scrivo a questo proposito il Garante Italiano nella "Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali" (pag.24-25) del luglio scorso:

"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."

E ancora:

"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'ammonizione del titolare fino alla limitazione o al divieto di procedere al trattamento."

Come si può constatare, dunque, grande libertà di decisione ma totale responsabilità a carico del Titolare o del Responsabile, nelle scelte intraprese. Con questa logica, le sanzioni previste possono raggiungere il 4% del fatturato globale dell'azienda giudicata inadempiente, con il massimo di 20.000.000,00 (ventimilioni/00) di euro!

SERVIZIMPRESA S.r.l.

Sede legale e Direzione di Chieri - Via Vittorio Emanuele II, 33 - 10023 Chieri (TO) - Tel + 39 011 9421694
Direzione di Rivoli - Corso Susa, 242 - 10098 Rivoli (TO) - Tel + 39 011 9535223

www.servizimpresa.it - info@servizimpresa.it - servizimpresa@pec.it

Cap.Soc. € 100.000,00 i.v. - C.F. / P.IVA / Iscr. Reg. Imprese 07646510011 • R.E.A. 908868



SERVIZIMPRESA s.r.l.

E' utile notare che:

- Deve essere possibile dare evidenza della metodologia adottata per l'analisi dei rischi;
- L'analisi dei rischi rappresenta la base di partenza per tutta una serie di adempimenti che saranno necessari ad ottemperare alla norma;
- Occorre definire e poter dimostrare la politica adottata dalla società nell'ambito dei trattamenti dei dati e le procedure operative applicate;
- Il Titolare o il Responsabile dovrà essere in grado di dimostrare che le politiche adottate rispondono ai criteri di sicurezza dettati dal Regolamento;
- La formazione degli incaricati sarà necessaria e dovrà essere veritiera e documentata;
- I riesami della direzione del sistema privacy saranno necessari per documentare l'attenzione e la manutenzione prestata al sistema privacy;
- I documenti utilizzati dovranno essere conformi alla normativa e riesaminati con regolarità;

La nostra soluzione

Per ottemperare alla nuova normativa reputiamo necessario predisporre il

"Dossier Privacy a norma del Regolamento Europeo 2016/679"

che dovrà contenere, tra l'altro:

- a) L'organigramma aziendale in ambito Privacy;
- b) Nuovo documento denominato "Sistema Privacy Aziendale" personalizzato che spiegherà la politica aziendale adottata nell'ambito delle procedure per protezione dei dati e che conterrà copia di tutti i documenti formali utilizzati dal Sistema Privacy;
- c) Le Schede analitiche dei trattamenti secondo gli standard in uso;
- d) Un'ampia descrizione dei sistemi informatici e delle misure di sicurezza adottate;
- e) Le credenziali per l'utilizzo del software specialistico, per la compilazione e la manutenzione dei "Registri dei trattamenti", della "Analisi e Valutazione dei rischi" e della Valutazione d'impatto;
- f) I "Registri della formazione", per l'evidenza dell'obbligo formativo;
- g) I contratti eventuali adottati per la figura del Responsabile esterno, dell'amministratore di sistema, del DPO, ecc.-;
- h) Le copie delle lettere di incarico firmate;
- i) La documentazione inerente le richieste e le autorizzazioni per la videosorveglianza e/o la geolocalizzazione, qualora in essere;
- j) Un eventuale programma di audit;
- k) Lo scadenziario delle verifiche, delle valutazioni del sistema di sicurezza e della formazione;
- l) I riesami della Direzione.

Le fasi (indicative e non esaustive) di attuazione del Sistema Privacy aziendale saranno le seguenti:

- Verificare l'organigramma attuale (responsabilità) e apportare eventualmente le necessarie variazioni;
- Formulare il documento personalizzato di Policy Aziendale
- Attivare le credenziali del software gestionale per la tenuta dei "Registri dei trattamenti", per l' "Analisi e Valutazione dei rischi" e per la eventuale "Valutazione d'impatto"
- Effettuare una coerente ed efficace "Valutazione dei rischi";



SERVIZIMPRESA s.r.l.

- Predisporre una descrizione specifica ed analitica dei trattamenti;
- Stabilire eventuali nuove procedure per il trattamento dei dati nel rispetto della Valutazione emersa;
- Formulare nuovi contratti con le figure di sistema (responsabili esterni, amministratori di sistema, ecc.-);
- Formulare le lettere di incarico dopo aver valutato gli ambiti di autorizzazione;
- Ridefinire e adottare nuove Informative e nuovi Consensi che andranno a sostituire i documenti attualmente in uso;
- Programmare una o più sessioni di formazione specifica per conoscere le regole e l'applicazione del nuovo Regolamento;
- Effettuare un Riesame della Direzione al fine di verificare, approvare e condividere le procedure adottate dal Sistema Privacy Aziendale;
- Formulare uno scadenziario per la revisione semestrale del Sistema Privacy Aziendale.

Questo in sintesi è l'approccio al Regolamento Europeo necessario e sufficiente per una corretta politica di gestione della Privacy con l'attuazione della nuova normativa.

Qualora il lettore sia interessato ad approfondire ed analizzare l'impatto privacy sulla propria realtà aziendale e definire un piano eventuale di intervento, verificandone i relativi costi, siamo disponibili per un incontro che potrà fissare chiamando ai riferimenti sotto indicati.

SERVIZIMPRESA SRL
Dott. Oscar Bernardi

Muriel Marmello: 011/9531785
Oscar Bernardi: 335/7031993