saltech+
SALUTE LAVORO TECNOLOGIA

Sezione Trattamento Dati

GDPR

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Cos'è il GDPR?

Il Regolamento Europeo n. 679/2016 sulla protezione dei dati personali, noto come **GDPR (General Data Protection Regulation)**, è entrato in vigore il 24 maggio 2016, e diverrà direttamente applicabile dal 25 maggio 2018 (termine ultimo di adeguamento), abrogando la Direttiva 95/46/CE.

Il nuovo quadro normativo prevede maggiori tutele nel trattamento dei dati personali, adempimenti più complessi e sanzioni più pesanti.
Il trattamento dei dati personali viene posto al centro delle organizzazioni aziendali ed in questo ambito sono previste nuove figure professionali.

Campo di applicazione

Il **General Data Protection Regulation**, impone a tutte le aziende e ai professionisti operanti nei Paesi membri della Ue una serie di novità di assoluto rilievo in materia di trattamento dei dati personali. Ove per trattamento dati deve intendersi *qualsiasi informazione riguardante una persona fisica identificata o identificabile* (quindi, ad esempio, sono dati personali: l'indirizzo di posta elettronica mariorossi@rossi.it, i dati anagrafici del Sig. Rossi, il suo numero di telefono …)

PRINCIPALI OBBLIGHI

Il GDPR introduce rispetto alla precedente normativa:

1.RESPONSABILIZZAZIONE DEL TITOLARE DEL TRATTAMENTO (ACCOUNTABILITY):

Il soggetto che determina le finalità e i mezzi del trattamento dei dati personali è definito titolare del trattamento e può essere una persona fisica o giuridica, un'autorità pubblica, un servizio o altro organismo.
Il suo compito è quello di porre in essere tutte le misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato conformemente al Regolamento.
Il titolare deve dimostrare la concreta **adozione di misure tecniche e organizzative adeguate** per garantire che il trattamento sia coerente alla norma. A tal fine il titolare deve rispettare i seguenti principi

- **Principio privacy by design**: il trattamento dei dati deve prevedere sin dall'inizio le garanzie indispensabili per tutelare i diritti e le libertà degli interessati.
- **Principio privacy by default**: ovvero la necessità di mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento.

PRINCIPALI OBBLIGHI

2.LICEITA' DEL TRATTAMENTO

Il Regolamento pone particolare attenzione al principio della liceità, correttezza e traspernza.
I fondamenti di liceità del trattamento sono:

- il consenso esplicito dell'interessato;
- l'adempimento di obblighi contrattuali;
- l'adempimento di obblighi legali cui è tenuto il titolare;
- la salvaguardia di interessi vitali per una persona fisica;
- interesse pubblico o esercizio di pubblici poteri;
- il perseguimento di un legittimo interesse del titolare o di terzi cui i dati vengono comunicati.

Non è ammesso il consenso tacito o presunto.
Il titolare del trattamento deve essere sempre in grado di dimostrare che l'interessato ha prestato il consenso al trattamento dei dati.

PRINCIPALI OBBLIGHI

3.INFORMATIVA

L’informativa deve essere fornita all’interessato prima di effettuare la raccolta dei dati.
Il titolare deve fornire all’interessato una lunga serie di informazioni, elencate in modo tassativo negli articoli 13 e 14 del Regolamento (qui non riportate per brevità).
Le informazioni che il titolare del trattamento deve fornire all’interessato devono sempre essere rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro.

PRINCIPALI OBBLIGHI

4.I DIRITTI DEGLI INTERESSATI E LE MODALITA' DI ESERCIZIO

Il GDPR disciplina il trattamento dei dati su cinque diritti fondamentali:

1. **Diritto di accesso:** si configura come il diritto del soggetto interessato di richiedere e ottenere dal titolare del trattamento le informazioni sul trattamento dei suoi dati personali.
2. **Diritto all'oblio:** ovvero il diritto dell'interessato a veder cancellati i dati personali che lo riguardano
3. Diritto di rettifica: il diritto dell'interessato di richiedere che siano modificati, corretti o aggiornati i dati che lo riguardano
4. **Diritto di limitazione** consiste nel diritto riconosciuto all'interessato di richiedere al titolare che il trattamento dei suoi dati sia limitato alla sola conservazione
5. **Diritto alla portabilità dei dati:** l'interessato ha il diritto di ricevere dal titolare copia dei dati personali oggetto del trattamento in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

4.I DIRITTI DEGLI INTERESSATI E LE MODALITA' DI ESERCIZIO

ove per interessato s'intende la persona fisica cui si riferiscono i dati personali (esempio: lavoratore dipendente, azienda cliente, persona fisica cliente).
In particolare si sottolinea che il titolare del trattamento è tenuto ad agevolare l'esercizio dei diritti dell'interessato. Qualora l'interessato faccia richiesta al titolare il termine di risposta è per tutti i diritti di 1 mese, estensibile 3 mesi in casi di particolare complessità.

PRINCIPALI OBBLIGHI

5.PRIVACY IMPACT ASSESSMENT

Per “valutazione d’impatto”, s’intende l’analisi dell’origine, della natura e della gravità del rischio per la tutela del diritto alla protezione del dato. Solo all’esito di tale valutazione il titolare potrà decidere se procedere con il trattamento dei dati secondo le misure che ha predisposto. Qualora lo ritenesse necessario potrà consultare le autorità di controllo per avere indicazioni sulla gestione del rischio residuale.

PRINCIPALI OBBLIGHI

6.DATA PROTECTION OFFICER

Il Regolamento introduce la figura del “Data Protection Officer” (DPO) o del “responsabile per la protezione dei dati” (RPD) al quale sono attribuiti importanti compiti ai fini della protezione dei dati e, in primo luogo, quello di sorvegliare l’osservanza del Regolamento.

Il Data Protection Officer deve avere una conoscenza specialistica della normativa e della prassi in materia di protezione dei dati e deve avere le capacità necessarie per assolvere i compiti di cui è investito.

PRINCIPALI OBBLIGHI

6.DATA PROTECTION OFFICER

La nomina del DPO è obbligatoria:

- ✓ quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (ad eccezione delle autorità giurisdizionali nell'esercizio di tali funzioni);
- ✓ ove i trattamenti, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- ✓ quando le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali (dati sensibili) o di dati relativi a condanne penali.

PRINCIPALI OBBLIGHI

7.RESPONSABILE DEL TRATTAMENTO

Il titolare del trattamento può designare un responsabile del trattamento, che tuteli i dati personali per suo conto. Questi deve prestare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale da garantire la tutela dei diritti dell'interessato.
L'affidamento del trattamento al responsabile deve avvenire con un contratto stipulato informa scritta e che disciplini tassativamente le materie indicate nel Regolamento.

PRINCIPALI OBBLIGHI

8.NOTIFICA VIOLAZIONE DATI PERSONALI (DATA BREACHES)

In caso di violazione dei dati personali, il titolare del trattamento deve notificare la violazione all'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

PRINCIPALI OBBLIGHI

9.REGISTRO DEI TRATTAMENTI

Il titolare deve tenere un registro delle operazioni di trattamento. Sebbene il GDPR escluda da tale obbligo i soggetti con meno di 250 dipendenti (solo se non effettuano trattamenti a rischio ovvero limiti i diritti e la libertà dell'interessato), il Garante della Privacy consiglia fortemente la sua tenuta da parte di tutti i soggetti che trattano dati personali poiché si tratta di uno strumento fondamentale per avere un elenco aggiornato di tutti i trattamenti effettuati.

MODALITA' OPERATIVE

In relazione alla necessità di adeguarsi al nuovo Regolamento Europeo si prevede la seguente modalità operativa:

1. PRIVACY ASSESTMENT nuova mappatura dei trattamenti e dei ruoli al fine di progettare l'implementazione di un Sistema di Governance della Privacy strutturato ed in grado di accrescere il livello di protezione dei dati e di consapevolezza nei trattamenti, con particolare attenzione:
   - ✓ identificazioni banche dati;
   - ✓ vulnerabilità e criticità dei trattamenti operati;
   - ✓ procedure e policy internet;
   - ✓ gestione e disciplina dei trattamenti
   - ✓ gestione e disciplina degli incaricati;
   - ✓ documentazione di sistema;
   - ✓ analisi del sistema informativo e delle misure di sicurezza implementate secondo disposizioni di legge

finalizzata alla definizione di una gap analysis atta ad evidenziare gli scostamenti rispetto alla messa in conformità al nuovo Regolamento su richiamato

MODALITA' OPERATIVE

2. Valutazione e definizione applicativa del principio "Privacy by Default e Privacy By Design" su cui si basa il nuovo Regolamento
3. Valutazione del rischio per i trattamenti svolti.
4. Identificazione, pianificazione e applicazione delle misure minime di sicurezza fisiche e logiche per la protezione del dato
5. Redazione documentazione di sistema (registro dei trattamenti, incarichi interni al trattamento, incarichi e nomine responsabili del trattamento esterno, incarichi tecnici, informative, ecc….)
6. Definizione e implementazione di attività correlate al "Data Breach" (violazione del dato) compresa la definizione del sistema di allerta
7. Formazione degli incaricati al trattamento
8. Nomina del DPO (qualora necessario)

SANZIONI

Il Regolamento prevede solo sanzioni amministrative pecuniarie.
Le sanzioni erogate devono essere in ogni singolo caso effettive, proporzionate e dissuasive.
In relazione alla tipologia di violazione sono state distinte due entità di sanzioni:

- ✓ sanzioni amministrative pecuniarie fino a 10.000.000 di euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (es. nel caso non vengono poste in essere adeguate misure di sicurezza dei dati);
- ✓ sanzioni amministrative pecuniarie fino a 20.000.000 di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (es. in caso di violazione dei principi di base del trattamento, comprese le condizioni relative al consenso).

Le singole legislazioni nazionali potranno prevedere sanzioni penali.

SERVIZI OFFERTI DALLA SALTECH

I nostri consulenti sono a vostra disposizione per:

- ✓ assistenza e consulenza al fine di adeguare, alla vigente normativa, il sistema di gestione dei dati;
- ✓ chiarimenti in relazione agli adempimenti normativi.

Per qualunque ulteriore informazione, quindi, inviato:

1. tutti i nostri clienti a contattare i propri consulenti al fine di verificare l'adeguatezza del proprio sistema
2. tutti i possibili interessati a mettersi in contatto con il numero: **06.37.51.82.34**

saltech+
SALUTE LAVORO TECNOLOGIA

Sezione Trattamento Dati

GDPR

FINE