GDPR

GENERAL DATA PROTECTION REGULATION

LISTA DI CONTROLLO PER VERIFICARE LO STATO DI COMPLIANCE

GIULIA GC CASACCI

NORMATIVA DI RIFERIMENTO

DIRETTIVA 95/46

DIRETTIVA 2002/58

CODICE PRIVACY – D. LGS. N. 196/2003

REGOLAMENTO EUROPEO 2016/679

REGOLAMENTO E-PRIVACY

RATIO

NE BIS IN IDEM

UNIFORMAZIONE

PROTEZIONE

AMBITO DI APPLICAZIONE

CHECK LIST 1 – 2 – 3

1. SEDE DEL CONTROLLER

UNIONE EUROPEA

EXTRA UNIONE EUROPEA

ART. 3 GDPR

Il Regolamento si applica al trattamento dei dati personali effettuato da un Controller o da un Processor, nell'Unione.

Non rileva il luogo del trattamento, ma la **sede** del Controller o del Processor

2. INTERESSATI

PERSONE FISICHE IN UNIONE EUROPEA

PERSONE FISICHE EXTRA UNIONE EUROPEA

ART. 3 GDPR

Il Regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, anche quando il Controller o il Processor non hanno sede nella UE, quando le attività riguardano:

- Offerta di beni o servizi anche gratuiti
- Monitoraggio del comportamento, se all'interno della UE

3. TRASFERIMENTO DATI

UNIONE EUROPEA

EXTRA UNIONE EUROPEA

Nella scelta dei servizi offerti da fornitori è fondamentale valutare anche questo aspetto, es. per Provider server e db.

CATEGORIE DI DATI

CHECK LIST 4 – 5 - 6

4. CATEGORIE DI DATI RACCOLTI

DATI PERSONALI

PARTICOLARI CATEGORIE DI DATI

- DATI SENSIBILI
- DATI GIUDIZIARI
- - DATI BIOMETRICI O GENETICI

4. CATEGORIE DI DATI RACCOLTI

DATO PERSONALE qualsiasi informazioni concernente una persona fisica identificata o identificabile

DATO SENSIBILE categoria particolare di dati che è idonea a rivelare origine razziale o etnica, stato di salute, orientamento religioso, orientamento sessuale, orientamento politico

5. CATEGORIE DI INTERESSATI

DIPENDENTI

CLIENTI

FORNITORI

POSSIBILI FUTURI CLIENTI

6. PROVENIENZA DEI DATI

DATI RACCOLTI DIRETTAMENTE DALL'INTERESSATO

DATI RACCOLTI DA TERZE PARTI

DATI RACCOLTI AUTOMATICAMENTE

DATI RACCOLTI DA PUBBLICI ELENCHI O REGISTRI

SOGGETTI E ORGANIGRAMMA PRIVACY

CHECK LIST 7 – 8

7. NOMINA PROCESSOR – RESPONSABILE DEL TRATTAMENTO

SI

NO

Persona fisica o giuridica che tratta dati per conto del Controller.
Può essere soggetto interno o esterno, ma deve essere nominato attraverso un **contratto scritto** i cui elementi obbligatori sono previsti dal GDPR.

Il **Controller** è la persona fisica o giuridica che determina modalità e finalità del trattamento.

7bis. NOMINA AMMINISTRATORE DI SISTEMA

SI

NO

Figura professionale, persona fisica, il cui ruolo è finalizzato alla manutenzione e alla gestione di un impianto di elaborazione e dei suoi componenti, ovvero delle reti o dei sistemi.
Registrazione dei log e verifica annuale sul loro operato.

8. NOMINA INCARICATI

SI

NO

Persona fisica che effettua il trattamento operando sotto la diretta autorità del Controller o del Processor.

REGISTRO TRATTAMENTO

Obbligatorio per chi ha più di 250 dipendenti e per chi effettua «trattamenti a rischio».

ACCOUNTABILITY

SCOPO DEL TRATTAMENTO

BASE GIURIDICA DEL TRATTAMENTO

ADEMPIMENTI CONTRATTUALI

OBBLIGHI DI LEGGE

INTERESSE LEGITTIMO PREVALENTE

CONSENSO

9. INFORMATIVA

SI

NO

Contenuto obbligatorio e tassativo previsto dal GDPR.
Deve essere concisa, trasparente, intellegibile e facilmente accessibile, deve inoltre essere fornita prima della raccolta dei dati.

10. FINALITA’ DEL TRATTAMENTO

CONTROLLO SUL LUOGO DI LAVORO

VENDITA O COMUNICAZIONE A TERZI DEI DATI RACCOLTI

COMUNICAZIONI PROMOZIONALI E COMMERCIALI

PROFILAZIONE

11. CONSENSO

SI, RACCOLTO E CONSERVATO

SI, RACCOLTO E NON CONSERVATO

NO, NON RACCOLTO

Deve essere libero, **specifico**, informato e inequivocabile.
Deve inoltre essere documentato e documentabile.

12. CONSERVAZIONE DATO

SI, PREVISTO TERMINE MASSIMO

NO, NON PREVISTO TERMINE MASSIMO

SI, PREVISTI CRITERI PER STABILIRE LA DURATA DELLA CONSERVAZIONE

DIRITTI DELL'INTERESSATO

CHECK LIST 13

19. STRUMENTI APPLICATIVI per GARANTIRE DIRITTI INTERESSATO

SI

NO

Il GDPR individua una serie di diritti riconosciuti all'interessato (diritto di accesso, diritto all'oblio, limitazione del trattamento, rettifica, modifica, etc..).
L'esercizio di tali diritti deve essere garantito, è previsto **1 mese** di tempo per evadere le richieste pervenute.

DATA BREACH e PROCEDURE DI COMUNICAZIONE

SI

NO

In caso di data breach, il Controller deve comunicare la violazione all'Autorità entro 72 dall'evento.
Se la violazione è grave, ossia mette a rischio i diritti e le libertà delle persone, va comunicata anche agli interessati.