GDPR - Audit Checklist

DATA PROTECTION GAP ANALYSIS

Fotografia della situazione attuale e redazione di una tabella con un elenco di tutte le attività svolte e da svolgere, valutazione della loro conformità al GDPR ed interventi da realizzare.

A. ESAME DELLE TIPOLOGIE DI DATI, DI TRATTAMENTI E DI INTERESSATI AL TRATTAMENTO

- Stai elaborando dati personali?
- Stai elaborando dati personali sensibili?
- I dati personali dei bambini vengono raccolti e trattati?
- I dati che stai trattando vengono conservati in archivi cartacei o elettronici? Cartacei-Elettronici-Entrambi
- E' stato redatto un elenco delle tipologie di dato trattato?
- In relazione ai dati trattati, sono state definite le finalità del trattamento?
- E' individuata la base giuridica (ad es., contratto, legge, standard internazionale, ecc.) di ciascun trattamento?
- E' stato definito il tempo di conservazione, gli eventi che ne determinano la cancellazione?

B. DESIGNAZIONI E SOGGETTI

- Il Titolare del Trattamento: è stato identificato?
- Il Responsabile/i della protezione dei dati: sono stati designati per iscritto? E' stato redatto un elenco?
- Qualora esista il contitolare del trattamento, è stato identificato? Esiste un contratto tra i contitolari?
- Qualora sia stato previsto, è stato designato con documento scritto il rappresentante del titolare del trattamento?
- Incaricati del Trattamento: sono stati individuati e designati dipendenti e collaboratori con istruzioni scritte? E' stato redatto un elenco distinto per categorie?
- Amministratori di Sistema. Sono stati designati con istruzioni scritte? E' stato redatto un elenco?
- Sono stati organizzati, per i soggetti, corsi di formazione in aula od online?

C. INFORMATIVE E CONSENSO

- L'informativa dipendenti, collaboratori e ruoli aziendali, inclusa diciture footer email, è stata predisposta o revisionata?
- L'informativa fornitori è stata predisposta o revisionata?
- Sono raccolte, attraverso il sito internet, informazioni personali di terzi?
- L'informativa sito, inclusa cookies, è stata predisposta o revisionata?
- I moduli per il consenso, incluso quello per il sito web, sono stati predisposti o revisionati?
- I moduli per il consenso sono stati redatti in forma chiara e di facile comprensione per gli interessati?
- Sono indicati il nome e i dati di contatto?

D. MODALITA' DI CONSERVAZIONE E ACCESSO AI DATI

- E' stato redatto un elenco delle sedi e degli ambienti in cui sono conservati documenti cartacei contenenti dati personali?
- Le aree o gli armadi di conservazione dei dati personali sono protetti? (Vedi sistemi di sicurezza e protezione)
- E' stato redatto un elenco dei dispositivi elettronici di archiviazione?
- I dispositivi elettronici ed i dati in essi contenuti sono adeguatamente protetti? (Vedi sistemi di sicurezza e protezione)
- E' stato redatto un elenco dei software e delle procedure di trattamento?
- E' stato redatto un elenco delle modalità di archiviazione?

E. POLICY E DISCIPLINARI INTERNI

- E' stato redatto un disciplinare interno per utilizzo di posta elettronica? (es. è consentito l'utilizzo dell'account di posta elettronica aziendale per uso personale?)
- E' stato redatto un disciplinare interno sulle procedure in caso di data breach?

- E’ stato redatto un disciplinare interno su procedure da svolgere in caso di esercizio dei diritti da parte dell’interessato?
- Esiste una politica / procedura documentata per la gestione delle richieste di accesso ai dati personali?
- I soggetti interessati sono forniti di un meccanismo per richiedere l'accesso alle informazioni detenute?
- Sono previste procedure e formazione per assicurare che i dati personali siano controllati e, se imprecisi, siano immediatamente rettificati?
- Le politiche sulla privacy incorporano informazioni sulla conservazione? Esistono procedure per l'archiviazione e la distruzione dei dati?
- Dove previsto, è stato predisposto un registro dei trattamenti?
- E’ stata prevista la redazione della valutazione d’impatto (DPIA)
- E’ prevista una periodica verifica di aggiornamento ed attualizzazione delle procedure organizzative e di sicurezza adottate?

F. SISTEMI DI SICUREZZA E DI PROTEZIONE

- Sono state assegnate credenziali di accesso (username e password) diversificate, rispondenti a criteri di adeguata robustezza e inviolabilità e per le quali è richiesta la variazione periodica’
- Esistono delle credenziali di supervisione, conosciute esclusivamente dall’amministratore di sistema?
- I dispositivi ed i sistemi per la conservazione e per il trattamento sono costantemente aggiornati?
- I dispositivi sono dotati di software antivirus configurato per l’aggiornamento costante e la scansione periodica?
- L’amministratore verifica costantemente l’esecuzione degli aggiornamenti dei sitemi e dei software di protezione?
- Vengono usati sistema di criptatura e pseudominizzazione?
- Esiste un dispositivo “Firewall” di ultima generazione?
- Esistono sistemi di salvataggio (backup) automatizzati?
- E’ adottato il sistema di backup 3-2-1 (almeno 3 copie dei dati, su 2 dispositivi diversi, conservando 1 copia al di fuori degli ambienti operativi)?
- E’ stabilita una procedura di ripristino totale dei sistemi (Disaster Recovery o Business Continuity)?
- Vengono effettuate periodicamente le procedure di simulazione di ripristino dei dati e dei sistemi?
- Sono, i dispositivi informatici, protetti e dotati di sistemi di continuità elettrica (UPS)?
- E’ verificata periodicamente l’efficienza e l’autonomia dell’UPS?
- Il sistema di posta elettronica aziendale è basato su un dominio di proprietà dell’azienda/studio?
- E’ adottato un sistema di filtraggio “antiSpam” per la posta elettronica?
- L’eventuale sito internet prevede aree ad accesso ristretto e controllato?
- Se sì, le credenziali fornite per l’accesso sono dotate di password robuste ed inviolabili?
- I documenti cartacei che contendono dati personali sono conservati all’interno di ambienti o mobili dotati di chiusura di sicurezza?
- I locali o gli ambienti di conservazione dei documenti cartacei sono dotati di sistemi di videosorveglianza?

CHECK LIST di verifica: il REGISTRO dei TRATTAMENTI del TITOLARE

N.	Quesito/requisito	Si	No
1	L'organizzazione ha un numero di dipendenti pari o superiore a 250?		
2	Sono effettuati trattamenti che possono presentare un rischio per i diritti e le libertà degli interessati?		
3	In caso di risposta negativa al quesito n. 1) ma affermativa al n. 2), il trattamento è occasionale?		
4	In caso di risposta negativa al quesito n. 1) ma affermativa al n. 2), il trattamento include "categorie particolari di dati di cui all'articolo 9, paragrafo 1 (che sono gli odierni dati sensibili, con l'aggiunta dei dati genetici e biometrici), o i dati personali relativi a condanne penali e a reati di cui all'articolo 10"?		
5	Contiene il registro il nome e i dati di contatto del titolare del trattamento?		
6	Sono indicati il nome e i dati di contratto, ove sussistenti: ...del contitolare del trattamento? ...del rappresentante del titolare del trattamento? ...del responsabile della protezione dei dati?		
7	Sono esplicitate le finalità dei trattamenti effettuati?		
8	Per ciascun trattamento sono individuate le categorie di interessati (ad es., dipendenti, clienti/utenti, fornitori, ecc.)?		
9	Per ciascun trattamento sono individuate le categorie di dati, sono cioè rintracciati: dati che rivelano l'origine razziale o etnica (art. 9)? dati che rivelano le opinioni politiche (art. 9)? dati che rivelano le convinzioni religiose o filosofiche (art. 9)? dati che rivelano l'appartenenza sindacale (art. 9)? dati genetici (artt. 4, par. 1, n. 13 e 9)? dati biometrici (artt. 4, par . 1, n. 14 e 9)? dati relativi alla salute (artt. 4, par. 1, n. 15 e 9)? dati relativi alla vita/orientamento sessuale (art. 9)? dati relativi a condanne penali e reati (art. 10)?		
10	Per ogni trattamento sono indicate le categorie di destinatari, cui i dati sono o saranno comunicati?		

11	Vi sono trattamenti in cui i dati sono comunicati a destinatari di Paesi terzi ovvero di organizzazioni internazionali?		
12	Contiene il registro l'indicazione dei trattamenti che includono i trasferimenti di dati personali verso un paese Terzo o un'organizzazione internazionale?		
13	In caso di risposta affermativa al quesito n. 12), il registro include l'identificazione del paese terzo o dell'organizzazione internazionale?		
14	In caso di risposta affermativa al quesito n. 11), per i trasferimenti di cui al secondo comma dell'articolo 49, il registro documenta le prescritte garanzie adeguate (per l'art. 49, comma 2, "Il trasferimento di cui al paragrafo 1, primo comma, lettera g) [che sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse], non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari?)		
15	E' individuata la base giuridica (ad es., contratto, legge, standard internazionale, ecc.) di ciascun trattamento?		
16	Detta base giuridica consente, per ciascun trattamento, di definire un tempo massimo di gestione/conservazione dei dati?		
17	Sono indicati i termini ultimi previsti per la cancellazione delle diverse categorie di dati?		
18	Sono descritte le misure di sicurezza tecniche e quelle organizzative di cui all'articolo 32, par. 1, tra cui, a titolo di esempio: la pseudonimizzazione e la cifratura dei dati personali? la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento? la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico? una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?		
19	Dette misure garantiscono un livello di sicurezza adeguato al rischio?		
20	Ha il titolare aderito ad un codice di condotta (art. 40) o ad un sistema di certificazione (art. 42)?		
21	In quale misura il detto codice di condotta/sistema di certificazione include adempimenti in materia di misure di sicurezza dei trattamenti?		
22	Il registro contiene l'informazione circa l'adesione del titolare al codice di condotta/sistema di certificazione?		

23	Esplicita il registro le misure tecniche ed organizzative implementate e riconducibili al codice di condotta e/o al sistema di certificazione		
24	Reca il registro la data della sua emissione?		
25	E' specificato se si tratta di prima emissione o di successiva revisione?		
26	E', il registro, sottoscritto dalla funzione che in base al sistema di procure e deleghe dell'organizzazione è deputata a farlo?		
27	E' stabilita la modalità di conservazione del registro?		
28	E' definito l'ambito di distribuzione interna del registro?		
29	E' individuata la funzione responsabile della conservazione e distribuzione interna del registro?		
30	Il titolare ha pianificato la revisione del registro?		