Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

ALLEGATO 2

CHECK LIST PER LA VALUTAZIONE E L'EVENTUALE IMPLEMENTAZIONE DI MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

-- NOVEMBRE 2022

Di seguito si fornisce un esempio di check list utile per poter valutare preliminarmente le misure di sicurezza sia tecniche che organizzative esistenti nella realtà aziendale esaminata (si veda il § 8 del documento). Tale check list dovrà essere integrata e completata dal Commercialista tenendo conto della tipologia dei dati trattati e dei rischi specifici connessi ai diritti e alle libertà dell'interessato.

Controllo degli accessi

Occorre impedire che i dati personali presenti su supporti e sistemi di elaborazione dati siano letti, copiati, modificati oppure cancellati illecitamente, e si deve provvedere affinché le persone autorizzate all'uso di un sistema di elaborazione dati possano accedere ai dati esclusivamente in base all'autorizzazione per l'accesso.

C'è una portineria / reception sempre presidiata per l'accesso all'edificio oppure agli uffici?
L'azienda è dotata di sistema di videosorveglianza?
È utilizzato un registro dei visitatori?
L'edificio / gli uffici sono protetti da un sistema di rilevamento delle intrusioni?
Sono presenti password personali / nome utente / protezione dell'accesso ai sistemi con cui sono trattati i dati personali di cui il committente è titolare?
Come sono concesse le autorizzazioni per l'accesso?
Per l'amministrazione dei sistemi esiste un account ADMIN indipendente che differisce dall'account utente individuale ed effettivo dell'amministratore di sistema?
Esistono dei parametri vincolanti per le password in azienda? In caso affermativo descriverne i requisiti.
Il sistema IT obbliga l'utente al rispetto dei predetti parametri sulla password?
Le persone autorizzate al trattamento utilizzano account condivisi per accedere ai dati personali?
I profili di accesso ai sistemi IT vengono riesaminati almeno una volta all'anno per verificare che siano corretti, secondo un principio di profilazione degli accessi che tenga conto del ruolo e delle responsabilità di ciascun utente/autorizzato al trattamento?
Le credenziali di accesso sono disattivate quando l'autorizzato al trattamento non ha più diritto di accedere ai dati personali (ad esempio, per cessazione del rapporto di lavoro o cambio di mansione)?
È stato impostato un blocco automatico dello schermo protetto da password?
Descrivere le misure adottate nel caso in cui la password sia stata perduta / dimenticata / violata.
Esistono sistemi di produzione e di test separati in caso di necessità di interventi di manutenzione ai sistemi?
In che modo i supporti dati non più necessari (chiavette USB, dischi fissi, CD-Rom, DVD / dischetti), su cui sono memorizzati i dati personali vengono smaltiti dall'azienda?
Come viene smaltita la documentazione non più necessaria contenente dati personali?

I dati personali sono memorizzati fisicamente su server gestiti dal titolare o da terzi?
La sala in cui è ubicato il server è protetta da sistema di rilevamento delle intrusioni e/o da un sistema di chiusura?
Descrivere le modalità di gestione di un eventuale accesso da remoto (VPN / IPSec):
C'è un limite al numero di tentativi di accesso da remoto non riusciti?
L'accesso da remoto viene disconnesso automaticamente dopo un certo tempo di inattività?
I sistemi con cui vengono trattati i dati personali di cui il committente è titolare sono protetti da firewall?
In caso di trasferimento di dati, la trasmissione è criptata / protetta tecnicamente?
Altro

Integrità e disponibilità

È necessario garantire che i dati personali siano protetti da modifica, distruzione o perdita accidentale, oltre che da accessi non autorizzati.

I sistemi IT sono tecnicamente protetti dalla perdita dei dati / accesso ai dati non autorizzato?
Esiste un piano di emergenza documentato (ad es. misure di emergenza in caso di difetti dell'hardware / incendio / perdita totale ecc.)?
È stata implementata una procedura di business continuity da seguire in caso di violazione dei dati personali?
Esiste un piano di backup documentato?
Con quale frequenza sono realizzati i backup dei sistemi?
Su quali strumenti è salvato il backup?
Dove vengono conservati i backup?
I dati di backup / i backup sono criptati?
I dati personali sono trattati in modo pseudoanonimizzato?
In caso come avviene la pseudoanonimizzazione?
I dati sono trattati in modo criptato?
In caso di trattamento in modo criptato, come avviene la cifratura?
I soggetti (interni o esterni) che si occupano di cybersecurity sono ben identificati?
Esistono linee guida e standard per la verifica regolare della sicurezza del trattamento dei dati?
I controlli / verifiche della sicurezza si svolgono con regolarità?
I sistemi IT, mediante i quali vengono trattati i dati personali, sono sottoposti, almeno una volta all'anno, a penetration test o vulnerability assessment?

Sono stati individuati i soggetti a cui comunicare i dati personali indicati nell'informativa art. 13 e 14 del GDPR?
È stato verificato che non vi è alcun trasferimento di dati fuori dalla UE?

Cancellazione e diritto di accesso

Alla scadenza dei termini di conservazione o cancellazione i dati personali devono essere cancellati conformemente alla normativa sulla protezione dei dati personali, ossia devono essere resi completamente irriconoscibili oppure anonimi, ad es. mediante rimozione dei riferimenti personali; devono inoltre essere garantiti i diritti di cui si parla nelle informative.

I termini di cancellazione sono documentati per ogni categoria di dati?
Come avviene la cancellazione dei dati personali?
I dati di un interessato possono essere cancellati su richiesta?
Su richiesta dell'interessato, può essere fornita una copia dei dati personali memorizzati che lo riguardano?
Ci sono di misure tecniche in grado di consentire anche la rettifica, l'aggiornamento e la limitazione del trattamento dei dati personali su richiesta del soggetto interessato?
L'azienda dispone di misure tecniche in grado di consentire la restituzione dei dati personali su richiesta e/o al termine di un contratto come titolare / responsabile?
Altro

Misure organizzative di carattere generale

L'organizzazione è tenuta a nominare un responsabile della protezione dei dati personali ai sensi dell'art. 37 del Regolamento?
Risulta nominato per iscritto un responsabile della protezione dei dati ai sensi dell'articolo 37 del Regolamento?
Tutti gli autorizzati al trattamento hanno ricevuto le istruzioni per il trattamento dei dati personali nel quale sono coinvolti mediante lettera di incarico?
I dipendenti che trattano i dati personali ricevono una formazione documentata in materia di protezione dei dati personali?
I dipendenti si impegnano alla riservatezza dei dati per iscritto?
L'azienda ha nominato dei responsabili (esterni)?
Come viene garantito che i responsabili implementino le disposizioni contrattuali e le relative direttive e misure di sicurezza?
È stato adottato il registro delle attività di trattamento? In caso affermativo, questo registro è sempre aggiornato?

Le informative art. 13 e 14 del GDPR sono previste per tutte le attività di trattamento?
Viene richiesto il consenso al trattamento dei dati personali quando ne ricorrono i presupposti giuridici?
Come viene archiviata la documentazione che attesta il rilascio del consenso?
Sono state adottate misure organizzative interne volte a prevenire / gestire eventuali violazioni in merito al trattamento di dati personali da parte degli autorizzati al trattamento dei dati personali (procedura di data breach)?
Esiste un indirizzo e-mail dedicato dove possono essere segnalate violazioni dei dati personali (procedura di data breach) e in generale esiste un regolamento aziendale di data breach?
Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale?
Esiste ed è mantenuto aggiornato in inventario dei data base e archivi cartacei presenti in azienda?
Esiste un Regolamento per l'utilizzo delle attrezzature informatiche?
Esiste una procedura interna per dare seguito all'esercizio dei diritti dell'interessato?
Altro.