SCHEDE PRATICHE

1. **L'ITAL QUALE TITOLARE DEL TRATTAMENTO DEI DATI.**

Ai sensi dell'art 4 par. 1, n. 7 GDPR (C74) il titolare del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Nel caso di società o associazioni è sempre l'ente giuridico - in nome del legale rappresentante *pro tempore* - ad essere qualificato titolare.

Il termine inglese "Data Controller" (Titolare del trattamento) ben si concilia con il carattere gestionale di colui che può determinare finalità e mezzi del trattamento. L'ITAL, anche tramite i suoi responsabili territoriali, le cui strutture territoriali di riferimento sono state all'uopo nominate quali responsabili del trattamento ex art. 28 GDPR (C81), sarà titolare del trattamento di tutte le informazioni che vengono allo stesso fornite dagli assistiti in virtù o in correlazione del mandato ricevuto.

Il GDPR prevede altresì la **figura dei contitolari del trattamento** (art. 26, C79) quando più titolari determinano congiuntamente le finalità e i mezzi del trattamento. In questi casi è necessario un esplicito accordo interno che definisca le rispettive responsabilità ed osservanza degli obblighi, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR;

Ai sensi dell'art. 4 par. 1, n. 8 del GDPR il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento. Il Titolare, nello svolgimento della propria attività, dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato.

L'ITAL, fra gli altri, ha provveduto a nominare tutte le strutture territoriali quali Responsabili del trattamento ex art. 28 GDPR.

Il registro delle attività di trattamento elenca le informazioni sulle caratteristiche dei trattamenti effettuati dal titolare del trattamento. Ogni titolare del trattamento di dati dovrà tenere un registro delle categorie/tipi di trattamento dei dati personali implementati sotto la sua responsabilità.

Tale obbligo non vige per le organizzazioni con meno di 250 dipendenti, a meno che il trattamento non includa un rischio per i diritti e le libertà delle persone interessate, si tratti di trattamento non occasionale o se si riferisca in particolare a dati sensibili (come è per il Patronato) o a dati relativi a condanne e reati. Il Patronato sarà quindi soggetto all'obbligo di istituire un registro delle attività dal momento che il trattamento dei dati personali non è di tipo occasionale e include categorie particolari di dati di cui all'art.

9 par. 1 GDPR. In ogni caso la detenzione del registro è fortemente consigliata, anche nel caso non vi sia l'obbligo, perché consente di mappare più chiaramente i trattamenti e di monitorare gli stessi ai fini del rispetto dei principi del GDPR e dei diritti degli interessati, oltre a risultare molto utile, ove occorra, per fornire prova dell'esatto adempimento all'obbligo adeguamento al principio dell'accountability.
Tale registro, in conformità con l'articolo 30 del GDPR, deve includere le seguenti informazioni:

- il nome e i dettagli di contatto del titolare, del contitolare, del responsabile, se del caso, del rappresentante del titolare e, laddove nominato, del responsabile della protezione dei dati (RPD/DPO);
- le finalità del trattamento;
- una descrizione delle categorie di dati trattati, nonché delle categorie di interessati;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari dei paesi terzi o organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo un'organizzazione internazionale, compresa l'identificazione del paese terzo o di tale organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49, i documenti che certificano l'esistenza di garanzie adeguate;
- ove possibile il termine ultimo previsto per la cancellazione dei dati;
- ove possibile una descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'articolo 32, par. 1.

Quali dati tratta il Patronato?

Il patronato tratta in via principale:

- i dati relativi al personale dipendente ed ai collaboratori;
- i dati relativi agli assistiti;
- i dati raccolti attraverso il sito internet.

a. I dati relativi ai dipendenti e ai collaboratori

Nell'ambito dei rapporti di collaborazione o di lavoro ivi inclusi la gestione del libro paga e la gestione amministrativa del personale, il Patronato, in qualità di datore di lavoro, effettua un trattamento di dati. Il trattamento deve essere effettuato in conformità alle norme del GDPR, ricordando che all'art. 88 è disposto che gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro. I dati trattati saranno unicamente quelli necessari alla corretta esecuzione del contratto nonché quelli il cui trattamento è necessario per adempiere gli obblighi legali ai quali è soggetto il titolare del trattamento, nel rispetto della normativa vigente.
Nel contesto della gestione dei suoi dipendenti il Patronato, in qualità di

datore di lavoro, può raccogliere principalmente due tipi di dati:
• Dati necessari per ottemperare a un obbligo legale.
• Dati utili per:
(i) gestione amministrativa del personale;
(ii) organizzazione lavoro.
Durante il colloquio per l'assunzione, i dati dovrebbero essere usati solo per valutare la capacità del candidato di eseguire il lavoro proposto. Potranno pertanto essere raccolti solo i dati relativi alla qualifica e all'esperienza del candidato (esempi: diplomi, precedenti lavori, ecc.).
È pertanto vietato: • raccogliere dati sulla famiglia del candidato; • raccogliere dati su opinioni politiche o appartenenza sindacale del candidato nonché qualsiasi dato classificato come particolare ai sensi dell'art. 9, par. 1 GDPR o comunque qualsivoglia dato, anche comune, non necessario rispetto alla finalità. Il Patronato potrebbe determinare le condizioni di utilizzo dell'accesso a Internet da parte di dipendenti e personale sul luogo di lavoro: può inserire i filtri per bloccare determinati contenuti (pornografia, pedofilia, ecc.). È anche possibile limitare l'uso di Internet per motivi di sicurezza, ad esempio il download di software, o predisporre strumenti atti a controllare le ore di lavoro o l'accesso da parte dei dipendenti ai files. Non è invece possibile estendere al controllo dell'attività dei dipendenti l'utilizzo di un eventuale software installato al fine di calcolare il tempo dedicato dal dipendente allo studio o alla predisposizione di atti di una pratica o strumenti similari. Per quanto riguarda i controlli datoriali sugli strumenti informatici aziendali è in ogni caso necessario il rispetto, oltre che della normativa sulla privacy, dell'art. 4 dello Statuto dei lavoratori.
In base al principio generale per cui il trattamento non può protrarsi oltre il tempo
necessario per l'espletamento degli incarichi, ovvero il tempo necessario in funzione della finalità del trattamento stesso, i dati relativi ai dipendenti o ai collaboratori potranno essere conservati per il tempo della durata del rapporto, aumentato dell'eventuale tempo di maturazione della prescrizione, al fine di far valere i diritti nascenti dal rapporto.
I dipendenti e i collaboratori del Patronato devono ricevere apposita informativa di cui all'art. 13 GDPR ed in particolare in merito a: • l'identità e i dati di contatto del titolare del trattamento; • i dati di contatto del responsabile della protezione dei dati laddove nominato; • le finalità del trattamento (gestione amministrativa del personale e assunzioni); • la base giuridica del trattamento; • interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. comma 1 lettera f; • destinatari dei dati (chi tiene i libri paga, ecc.); • l'eventuale intenzione del titolare di trasferire dati a un paese terzo o a un'organizzazione internazionale e a tal proposito, in caso di assenza di una decisione di adeguatezza della Commissione, il riferimento alle garanzie adeguate; • il periodo di

conservazione; • l'esistenza dei diritti di accesso, rettifica, cancellazione, limitazione del trattamento ovvero di opposizione ed il diritto di portabilità dei dati; • Il diritto di revocare il consenso se è la base giuridica del trattamento senza per questo pregiudicare la liceità del trattamento pregresso; • Il diritto di presentare un reclamo all'autorità di controllo (in Italia, Autorità per la protezione dei dati personali); • se la comunicazione dei dati è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione del contratto; • l'eventuale esistenza di un processo decisionale automatizzato.
Questa informazione può essere inserita nell'accordo di collaborazione o nel contratto di lavoro, ovvero può essere oggetto di documento visualizzato o può essere inviata comunicazione via e-mail, in particolare per regolarizzare la situazione con dipendenti e personale che non sono stati adeguatamente informati.

RIASSUMENDO:
COSA DEVE FARE IL PATRONATO?
1. VERIFICARE CHE I DATI RACCOLTI SIANO ESCLUSIVAMENTE QUELLI NECESSARI RISPETTO ALLA FINALITÀ DEL TRATTAMENTO;
2. VERIFICARE CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI;
3. RISPETTARE I PRINCIPI DI CUI ALL'ART. 5 GDPR;
4. VERIFICARE I DISPOSITIVI DI CONTROLLO DELL'ATTIVITA' DEL PERSONALE, LA LORO PERTINENZA ED IL RISPETTO DELLA NORMATIVA VIGENTE
5. INSERIRE I DATI RELATIVI AL TRATTAMENTO NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto)
6. DEFINIRE LA DURATA DI CONSERVAZIONE DEI DATI
7. DARE L'INFORMATIVA AGLI INTERESSATI

******

b) I dati relativi agli assistiti
Nell'ambito dell'esercizio della propria attività istituzionale di patronato, il trattamento dei dati personali dell'assistito riguarda tutti i dati necessari per la presentazione delle domande tese ad ottenere i benefici assistenziali e previdenziali e per la difesa, anche giudiziale dei relativi interessi. Data la diversità dei campi di intervento, questi dati possono essere molto diversi fra loro e possono essere relativi alla vita personale dell'assistito, ivi inclusi dati particolari di cui all'art. 9 par. 1 GDPR: il patronato, infatti, potrebbe avere a che fare con dati personali che rivelano l'origine razziale o opinioni etniche, politiche, credenze religiose, l'appartenenza sindacale, così come l'elaborazione di dati genetici, dati biometrici, dati sanitari unici o di vita, orientamento sessuale. L'articolo 9, comma 1 del GDPR prevede il divieto in linea di principio del trattamento di tali dati eccetto i casi di cui al

paragrafo 2 del medesimo articolo 9. In particolare, all'art. 9, par. 2, lett. a) è disposto che il trattamento dei dati particolari non è vietato laddove l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche; sempre l'art. 9, par. 2, lett. f) stabilisce la liceità del trattamento dei dati particolari nel caso in cui il trattamento sia necessario per "*accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali*".

Il Patronato può quindi trattare dati particolari laddove abbia ricevuto esplicito consenso da parte dell'interessato (assistito) ovvero nel caso in cui i dati particolari siano strettamente necessari per esercitare o difendere i diritti propri o degli assistiti in giudizio. Ovviamente è raccomandata una interpretazione rigorosa di questa necessità.

L'art. 116, D. Lgs. 196/2003 stabilisce altresì che "per lo svolgimento delle proprie attività, gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato (dall'interessato medesimo).

In tema di trattamento di dati particolari da parte degli istituti di patronato si richiama altresì l'Autorizzazione n. 3/2016 – autorizzazione al trattamento di dati sensibili da parte degli organismi di tipo associativo e delle fondazioni del 15.12.20216, unitamente al Provvedimento del 13.12.2018 che individua le prescrizioni contenute nelle autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/016 e 9/2016 che risultano compatibili con il Regolamento e con il d. lgs. 101/2018 di adeguamento del Codice nonché il Provvedimento in tema di autorizzazioni generali del Garante per la protezione dei dati personali del 19.07.2018.

E' opportuno che il trattamento di dati particolari effettuato dal Patronato, in quanto non occasionale, sia previsto nel registro dei trattamenti in apposito modulo che deve includere i seguenti elementi: ● Identità e dettagli di contatto del titolare del trattamento; ● Scopi; ● Categorie di persone interessate; ● Categorie di dati personali; ● Categorie di destinatari; ● Trasferimenti verso un paese terzo o un'organizzazione internazionale; ● Termine finale del trattamento; ● Descrizione generale delle misure di sicurezza tecniche e organizzative.

Informativa agli assistiti

In conformità con quanto previsto all'13 del GDPR, gli assistiti devono essere informati su: • l'identità e i dettagli di contatto del titolare del trattamento ; • i dati di contatto del responsabile della protezione dei dati laddove nominato; • le finalità del trattamento (corretta esecuzione del mandato di assistenza conferito, ivi inclusa la gestione ed il monitoraggio dei file degli assistiti); • la base giuridica del trattamento (prestazione contrattuale o precontrattuale su richiesta dell'assistito ed esplicito

consenso per il trattamento di dati particolari anche idonei a rivelare lo stato di salute da parte di quest'ultimo); • interesse legittimo del titolare se costituisce la base giuridica del trattamento ex art. 6. comma 1 lettera f; • destinatari dei dati; • l'eventuale intenzione del titolare di trasferire dati a un paese terzo o a un'organizzazione internazionale e a tal proposito, in caso di assenza di una decisione di adeguatezza della Commissione il riferimento alle garanzie adeguate; • il periodo di conservazione; • l'esistenza dei diritti di accesso, rettifica, cancellazione, limitazione del trattamento ovvero di opposizione, ed il diritto di portabilità dei dati; • il diritto di revocare il consenso se è la base giuridica del trattamento senza per questo pregiudicare la liceità del trattamento pregresso; • il diritto di presentare un reclamo all'autorità di controllo (in Italia, Autorità per la protezione dei dati personali); • se la comunicazione dei dati è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione del contratto; nel caso di specie affinché l'istituto di Patronato possa correttamente svolgere la propria attività, la comunicazione dei dati è requisito necessario • l'eventuale esistenza di un processo decisionale automatizzato.
Queste informazioni devono essere incluse nel mandato di assistenza conferito dall'assistito ed in particolare mediante un'informativa breve, unitamente ai relativi consensi (obbligatori e facoltativi) in calce al mandato di assistenza; mediante un'informativa estesa allegata al predetto mandato; reperibili nell'apposita sezione dedicata alla privacy sul sito internet dell'ITAL nonché affissi nelle sedi di patronato; possono anche essere comunicate via e-mail, in particolare per regolarizzare la situazione con gli assistiti nella residuale eventualità in cui non siano stati adeguatamente informati.

Per quanto tempo devono essere conservati i dati dell'assistito?
Il Patronato, titolare del trattamento, deve definire una politica di durata e di conservazione dei dati nel suo ufficio. I dati personali possono essere conservati solo per il tempo necessario per il completamento dell'obiettivo perseguito durante la loro raccolta. In generale, i dati degli assistiti possono essere tenuti per la durata del mandato professionale. I dati dovranno essere conservati inoltre, prima della loro cancellazione definitiva, sino a che un'eventuale azione di responsabilità professionale, in cui potrebbe essere implicato il Patronato, non sia prescritta.
Cosa deve fare il Patronato in caso di revoca del mandato?
Come già rilevato più sopra con riferimento al diritto di portabilità dei dati, il Patronato che ha inizialmente trattato i dati è tenuto a comunicare all'assistito i dati da quest'ultimo forniti in un formato strutturato, di uso comune e leggibile da dispositivo automatico, qualora:
- il trattamento si basi sul consenso ai sensi dell'art. 6, par. 1, lett. a) o dell'art. 9, par. 2, lett. a), o su un contratto ai sensi dell'art. 6, par. 1, lett. b) e il trattamento

è stato effettuato con mezzi automatizzati.
Pertanto, se l'assistito richiede la trasmissione dei suoi dati ad un altro patronato, l'ITAL dovrà trasferirli in formato strutturato comunemente usato e leggibile da una macchina.

La sicurezza del fascicolo telematico e\o cartaceo.

È necessario adottare misure e procedure di sicurezza adeguate alla sensibilità dei dati coinvolti nei trattamenti. Per fare ciò, è necessario verificare che l'accesso ai locali in cui sono conservati o memorizzati i fascicoli sia sufficientemente sicuro (a titolo esemplificativo: uffici o relativi armadi chiusi a chiave; accesso ad aree in cui sono conservati i documenti mediante badge o comunque limitato a personale appositamente autorizzato; ecc.). È altresì di primaria importanza verificare la sicurezza del sistema informatico sul quale i file sono memorizzati in formato digitale (firewall, password robuste per accesso, diritti, ecc.)

RIASSUMENDO:

COSA DEVE FARE IL PATRONATO?

1. VERIFICARE CHE I DATI RACCOLTI SIANO SCLUSIVAMENTE QUELLI NECESSARI ALL'ESATTA ESECUZIONE DEL MANDATO RICEVUTO E NON SIANO ECCESSIVI RISPETTO ALLA FINALITÀ DEL TRATTAMENTO;
2. VERIFICARE CHE CI SIA UNA BASE LEGALE PER IL TRATTAMENTO DEI DATI;
3. RISPETTARE IL PRINCIPIO DI MINIMIZZAZIONE;
4. DEFINIRE LA DURATA DI CONSERVAZIONE DEI DATI;
5. INSERIRE I DATI NEL REGISTRO DI TRATTAMENTO DEI DATI (ove tenuto);
6. VERIFICARE CHE I FASCICOLI DEGLI ASSISTITITI TANTO DIGITALI CHE CARTACEI SIANO CONSERVATI IN MODO SICURO;
7. VERIFICARE LA SICUREZZA DEL SISTEMA INFORMATICO CON IL FORNITORE APPOSITAMENTE NOMINATO QUALE AMMINISTRATORE DI SISTEMA.

***

LA FIGURA DEL RESPONSABILE DEL TRATTAMENTO

Ai sensi dell'art. 4, par. 8 **il responsabile del trattamento** è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che "tratta dati personali per conto del titolare del trattamento".
È importante sottolineare il concetto del trattamento dei dati personali **"per conto" del titolare del trattamento**.
Il responsabile, in sostanza, effettua il trattamento in quanto i dati personali gli sono comunicati dal titolare del trattamento. In pratica, è la persona fisica o giuridica che tratta dati personali per conto del PATRONATO come ad esempio un consulente, un contabile, un editore di software, un host

web, ecc.

I soggetti che trattano dati personali per conto del Patronato sono appositamente nominati dallo stesso quali responsabili del trattamento (es.: commercialista, consulente del lavoro, consulente medico, fornitori di servizi digitali, conservatori di documenti informatici, ecc.). Nella ipotesi in cui vi sia un responsabile del trattamento (un soggetto esterno) e qualora fosse una persona fisica, la prima cosa da fare è fornire l'informativa al momento della raccolta dei suoi dati personali. Nel caso di persone giuridiche si può procedere con la sottoscrizione del contratto.

L'art. 28, par. 3, del GDPR prevede l'obbligo di stipulare un contratto tra titolare e responsabile del trattamento, i cui elementi necessari sono previsti nel medesimo art. 28 . Fra gli altri, il contratto dovrà includere: • la materia disciplinata; • la durata del trattamento; • natura e finalità del trattamento; il tipo di dati personali coinvolti; le categorie di persone interessate; • i diritti e gli obblighi del titolare del trattamento; • le misure di sicurezza adottate in relazione al trattamento dei dati che sarà effettuato.

Il contratto deve anche definire ulteriori obblighi del responsabile quali:

- la possibilità di elaborare dati solo su istruzione documentata del titolare del trattamento anche in caso di trasferimento dei dati in paesi terzi o verso organizzazioni internazionali;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un obbligo legale di riservatezza;
- adottare tutte le misure richieste ai sensi dell'art. 32;
- rispettare le prescrizioni di cui al medesimo art. 28 in caso di nomina di altro responsabile del trattamento;
- affiancare e coadiuvare il titolare, con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del titolare di dar seguito alle richieste di esercizio dei diritti delle persone interessate;
- assistere il titolare nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile;
- su scelta del titolare, dar seguito alla cancellazione o alla restituzione dei dati in questione una volta cessato il trattamento, salvo il caso in cui la loro conservazione sia richiesta da una disposizione nazionale o europea;
- mettere a disposizione del titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi e consentire le attività di verifica, comprese le ispezioni, da parte del titolare o di suo incaricato e collaborando in queste attività di audit;
- l'eventuale assunzione da parte del responsabile di altro responsabile per l'esecuzione di specifiche attività di trattamento per conto del titolare, nel rispetto di quanto previsto all'art. 28 GDPR, come di seguito specificato.

L'incarico deve essere formalizzato in un contratto che preveda almeno tutti gli obblighi sopra elencati e richiamati al medesimo art 28

GDPR. Le clausole contrattuali che vincolano titolari e responsabili devono pertanto essere molto precise sia sulle modalità di trattamento che sulla gestione delle loro relazioni e sullo scambio di informazioni tra di loro. Ai sensi dell'articolo 28, paragrafo 1, del GDPR il responsabile del trattamento dei dati ha l'obbligo di incaricare solo responsabili "che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".
Il GDPR stabilisce (art. 28, par. 2, GDPR) che il responsabile può nominare a sua volta un responsabile **(sub responsabile)** ma tale nomina è subordinata a esplicita autorizzazione scritta del titolare del trattamento.
Ai sensi dell'art. 29 del GDPR "Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

RIASSUMENDO:
COSA DEVE FARE IL PATRONATO RISPETTO AI RESPONSABILI DEL TRATTAMENTO?

1. IDENTIFICARE I RESPONSABILI DEL TRATTAMENTO;
2. VERIFICARE CHE I RESPONSABILI INDIVIDUATI PRESENTINO GARANZIE ADEGUATE;
3. VERIFICARE CHE I RESPONSABILI ALL'UOPO NOMINATI RISPETTINO LE PRESCRIZIONI OGGETTO DEL CONTRATTO STIPULATO CON IL TITOLARE A NORMA DELL'ART. 28 GDPR;
4. MODIFICARE E TENERE SEMPRE AGGIORNATO, OVE NECESSARIO IL CONTRATTO GIÀ ESISTENTE.

***

L'ADOZIONE DI BUONE PRASSI PER LA SICUREZZA DEI DATI

Come già si è detto, è essenziale garantire la sicurezza e la riservatezza dei dati trattati, garantendo un livello di sicurezza adeguato al rischio di trattamento.
In caso di documenti o fascicoli analogici è necessario mettere in atto misure di sicurezza fisica quali, a titolo esemplificativo: • Limitare gli accessi agli uffici a personale autorizzato; • Non archiviare fascicoli o documenti contenenti dati personali in locali accessibili a tutti; • Installare gli allarmi nei locali dell'ufficio.
In caso di documenti o fascicoli gestiti digitalmente si consiglia di: • Autenticare gli utenti: impostare una password minima di 8 caratteri contenenti maiuscole, lettere minuscole, numeri e caratteri speciali; non condividerla; non scriverla su fogli o post-it incustoditi; aggiornarla periodicamente; evitare la pre-registrazione; istruire gli utenti: determinare

persone che hanno il diritto di accedere ai dati personali; rimuovere le autorizzazioni di accesso obsolete; scrivere un regolamento di utilizzo del computer e inserirlo nel regolamento interno; • mobile computing sicuro: fornire mezzi di crittografia per computer portatili e dispositivi di archiviazione rimovibili (chiavette USB, CD, DVD ...), evitare di memorizzare dati personali sensibili di assistiti laddove non strettamente necessario alla corretta esecuzione dell'incarico • eseguire il backup e pianificare la business continuity: implementare i backup regolarmente, conservare i supporti di backup in un luogo sicuro, ecc.
Il titolare adotterà specifiche procedure atte allo scopo.

RIASSUMENDO:
COSA DEVE FARE IL PATRONATO?

MISURE DI SICUREZZA FISICHE

1. LIMITARE L'ACCESSO AI LOCALI A PERSONALE AUTORIZZATO;
2. VERIFICARE E METTERE IN SICUREZZA I LUOGHI OVE SONO CONSERVATI I FASCICOLI;
3. INSTALLARE SISTEMI DI ALLARME;

MISURE DI SICUREZZA DIGITALI

1. PREVEDERE MISURE DI IDENTIFICAZIONE DELL'UTILIZZATORE;
2. GESTIRE LE ABILITAZIONI E SENSIBILIZZARE L'UTILIZZATORE;
3. METTERE IN SICUREZZA I DISPOSITIVI, ANCHE MOBILI;
4. EFFETTUARE IL CENSIMENTO DEGLI ASSET (BENI FISICI O DIGITALI) UTILIZZATI NEL TRATTAMENTO DEI DATI;
5. EFFETTUARE LA VALUTAZIONE DEI RISCHI CONNESSI A CIASCUN ASSET E ADOTTARE LE RELATIVE CONTROMISURE;
6. PIANIFICARE LA BUSINESS CONTINUITY;
7. ADOTTARE UN REGOLAMENTO DI UTILIZZO DEL COMPUTER;
8. ADOTTARE PROCEDURE DI NOTIFICAZIONE DELLE VIOLAZIONI DEI DATI PERSONALI.

Il titolare adotterà specifiche procedure atte allo scopo.

In merito ai dati raccolti attraverso la navigazione del sito internet si rimanda all'apposita informativa. Si rappresenta come tutta la documentazione, ivi comprese prassi, procedure e linee guida inerenti la sicurezza dei dati trattati con strumenti elettronici ed informatici verrà predisposta con l'ausilio e la supervisione dei tecnici informatici all'uopo nominati quali amministratori di sistema.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI - DPO

Ai sensi dell'articolo 37 del GDPR, i titolari del trattamento e i responsabili dovranno nominare un responsabile della protezione dei dati ogniqualvolta:

- il trattamento sia effettuato da un'autorità, un organismo ovvero un ente

pubblico;

- le attività principali del titolare del trattamento e del responsabile del trattamento richiedano il monitoraggio regolare e sistematico degli interessati su larga scala;
- se le loro attività principali (core business) li portano a trattare (su larga scala) categorie specifiche di dati, noti come dati "sensibili" e dati su condanne penali e reati.

Negli altri casi, la nomina di un responsabile della protezione dei dati è ovviamente possibile, come opzione organizzativa ulteriore e di maggior cautela. In determinati casi i titolari del trattamento possono optare per un responsabile per la protezione di dati condiviso con altri, ovvero per un delegato interno all'organizzazione od esterno.

Il gruppo di lavoro articolo 29 (WP29), composto da rappresentanti delle Autorità Nazionali per la protezione dei dati degli Stati membri dell'UE ha pubblicato linee guida sul ruolo dei responsabili della protezione dei dati e fornito raccomandazioni per adottare buone prassi.

Il Patronato ha provveduto alla nomina di un responsabile della protezione dei dati, inserendone i dati di contatto nelle relative informative e comunicandone i dati all'autorità di controllo competente.

La previsione dell'art. 37 (così come quella dell'art 35) si applica sempre al titolare o al responsabile del trattamento riferito a categorie di dati particolari.

Queste disposizioni richiedono la nomina del DPO nei casi in cui le attività principali del titolare o del responsabile consistono in un trattamento su larga scala delle categorie di dati di cui all'articolo 9 GDPR.

Secondo le linee guida dei responsabili della protezione dei dati, "per "attività
principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare del trattamento o del responsabile del trattamento.

Va inoltre correttamente interpretata l'espressione "larga scala".

Vale, in ogni caso, la medesima regola espressa per la DPIA (documento di valutazione di impatto per la protezione dei dati): anche quando non obbligatoria, la designazione di
un Data Protection Officer potrebbe essere valutata come un'opportunità organizzativa nell'ormai imprescindibile gestione dei trattamenti.

Il titolare del trattamento si assicura che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati.

Il titolare sostiene il DPO nell'esecuzione dei compiti di cui all'art. 39 GDPR fornendogli le risorse necessarie per assolvere tali compiti.

Il titolare ed il responsabile del trattamento si assicurano che il DPO non riceva alcuna istruzione per l'esecuzione dei suoi compiti.

Il GDPR impone ai DPO degli obblighi importanti: sono come dei direttori di orchestra della conformità e adeguatezza in materia di protezione dei dati personali in seno alla struttura che li ha nominati.
Il DPO ha il compito precipuo di:

- Informare e fornire consulenza al titolare o al responsabile e ai loro dipendenti autorizzati al trattamento;
- Se richiesto, fornisce anche un parere sulla valutazione di impatto;
- Collaborare con il Garante ed essere il punto di contatto fra questo ed il titolare;
- È il punto di contatto per gli interessati del trattamento;
- Collaborare nell'adeguamento della struttura agli obblighi imposti dal regolamento europeo, fornendo informazioni sul contenuto dei nuovi obblighi imposti dal regolamento europeo e dalla normativa vigente;
- Condurre un inventario del trattamento dei dati della propria organizzazione;
- Progettare azioni di sensibilizzazione;
- Gestire in maniera continuativa la conformità dell'organizzazione al Regolamento.

Le responsabilità che sorgono in capo alla persona designata come DPO sono quindi rilevantissime.

DATA BREACH

In virtù degli artt. 33 e 34 del GDPR il Patronato che agisce quale titolare del trattamento deve notificare le violazioni dei dati personali al Garante, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche e comunicare la medesima violazione alle persone interessate in caso di rischio elevato per i diritti e le libertà personali. La violazione dei dati personali, il c.d. data breach, è una violazione della sicurezza che comporta accidentalmente o illecitamente, distruzione, perdita, alterazione, divulgazione o accesso non autorizzati di dati di natura personale trasmessi, conservati o altrimenti elaborati. Il titolare del trattamento ha l'obbligo di documentare - e di esibire ad eventuale richiesta del Garante – per qualsiasi violazione dei dati personali, le circostanze che l'hanno causata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Se il titolare si è avvalso di un responsabile del trattamento, quest'ultimo ha l'obbligo di notificare al titolare, senza ingiustificato ritardo dal momento in cui ne viene a conoscenza, qualsiasi violazione dei dati personali. È raccomandabile che tale obbligo sia oggetto di una specifica clausola contrattuale con il responsabile. In ottemperanza agli artt. 33 e 34 del GDPR il Patronato che agisce quale titolare del trattamento, in caso di elevata probabilità di rischio dei diritti e delle libertà personali, deve notificare al Garante e comunicare agli interessati le violazioni dei dati personali di cui viene a conoscenza. In applicazione del principio generale di accountability, è rimessa al titolare del trattamento la valutazione circa il fatto che lo specifico data breach possa presentare un rischio per i diritti e le libertà degli assistiti/ interessati.
Laddove la valutazione abbia esito affermativo, non oltre le 72 ore dalla presa

di coscienza (GDPR, Art. 33) il titolare del trattamento deve notificare la violazione al Garante per la protezione dei dati personali (in qualità di autorità competente), specificando, tra l'altro: ● la natura della violazione dei dati personali (categorie e numero approssimativo di persone e record di dati coinvolti dalla violazione); ● i dati di contatto del DPO (laddove applicabile); ● le probabili conseguenze della violazione; ● le misure adottate o da adottare per mitigare qualsiasi conseguenza negativa. Il modulo e la procedura per la notifica – solo online – della violazione dei dati personali è a disposizione del titolare sul sito del Garante.
Si raccomanda inoltre di: ● mettere in atto misure per analizzare i rischi del trattamento istituito per i diritti e le libertà delle persone fisiche; ● assicurarsi che le violazioni siano notificate entro 72 ore, in caso contrario spiegare accuratamente le motivazioni del ritardo all'autorità garante; ● indicare nella notifica i fatti della violazione, la natura della violazione, i suoi effetti e le misure adottate per porvi rimedio; ● fare ogni sforzo per documentare il più possibile qualsiasi violazione per consentire all'autorità di vigilanza di verificare la conformità ai requisiti imposti dal GDPR; ● mettere immediatamente in atto misure di emergenza per porre rimedio alla violazione e mitigare le conseguenze.
Laddove il titolare valuti che sia probabile che la violazione sia suscettibile di presentare un elevato rischio per i diritti e le libertà di una persona fisica, sarà necessario comunicare anche all'interessato il data breach. Tale comunicazione deve contenere almeno: ● i dati di contatto del DPO (ove applicabile); ● la descrizione - con un linguaggio semplice e chiaro - della natura della violazione dei dati personali e delle probabili conseguenze, le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi. La comunicazione all'interessato può non essere necessaria se: le misure tecniche e organizzative preventivamente approntate dal titolare abbiano reso i dati incomprensibili per qualsiasi persona; ciò capita, ad esempio, quando tali dati, pur diffusi, sono stati cifrati o crittografati; ● sono state adottate misure per garantire che il rischio sia scongiurato e non possa più verificarsi ● la comunicazione richieda "sforzi sproporzionati", ma in questo caso è autorizzata una comunicazione "pubblica" piuttosto che diretta sempreché la stessa possa raggiungere ed informare gli interessati con analoga efficacia della comunicazione diretta. La comunicazione agli interessati può anche essere richiesta dall'Autorità garante se quest'ultima reputa, dopo aver esaminato la notificazione, che vi sia un alto rischio per gli interessati derivante dal data breach.

RIASSUMENDO:
COSA DEVE FARE IL PATRONATO IN CASO DI DATA BREACH:

1. AVVISARE SENZA INDUGIO LE PERSONE COMPETENTI E LADDOVE NOMINATO, IL DPO;
2. QUALIFICARE LA VIOLAZIONE;
3. ADOTTARE LE MISURE NECESSARIE PER MINIMIZZARE LE CONSEGUENZE;
4. EFFETTUARE LE NOTIFICAZIONI ALL'AUTORITÀ GARANTE, A MENO CHE NON SIA IMPROBABILE CHE SUSSISTA UN RISCHIO PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE;
5. SE IL RISCHIO È ELEVATO EFFETTUARE LE COMUNICAZIONI AGLI INTERESSATI COINVOLTI;
6. IN OGNI CASO ANNOTARE TUTTE LE VIOLAZIONI (ANCHE SE NON NOTIFICATE) NEL REGISTRO DELLE VIOLAZIONI.

***

LE SANZIONI

Titolari e responsabili del trattamento possono essere soggetti a sanzioni amministrative significative per il mancato rispetto delle disposizioni del GDPR.
L'autorità Garante per la protezione dei Dati personali, può, in particolare:

- rivolgere avvertimenti;
- ammonire IL PATRONATO;
- limitare temporaneamente o permanentemente un trattamento;
- sospendere i flussi di dati;
- ordinare di soddisfare richieste per l'esercizio dei diritti delle persone;
- ordinare la rettifica, limitazione o cancellazione dei dati;
- può inoltre ritirare la certificazione di conformità concessa ovvero ordinarne il ritiro all'autorità di certificazione;
- comminare una elevata sanzione amministrativa.