**Sistema di data protection: l’importanza della documentazione**

I titolari del trattamento non solo sono tenuti a mettere in atto misure adeguate ed efficaci ma devono anche essere in grado di dimostrare la conformità delle attività di trattamento con lo stesso GDPR.

In concreto, questa mission deve essere trasfusa in un SGP – sistema di gestione privacy, cioè un sistema di documenti, regole, formazione e procedure di controllo omogeneo ed integrato, in altre parole armonioso. Caratteristiche peculiari: un SGP deve prevedere il suo aggiornamento in relazione all’evoluzione del contesto, garantendo comunque l’efficacia e l’efficienza dei processi aziendali.

Comunque, tutte le attività di trattamento dei dati personali, fin dalla progettazione, devono essere comprovate mediante la produzione, l’aggiornamento e la conservazione di adeguata documentazione.

Va innanzitutto precisato che per **documento** si intende ogni rappresentazione grafica, informatica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, fatti o dati giuridicamente rilevanti; anche interni o non, relativi ad uno specifico processo aziendale o procedimento amministrativo[[5]](https://www.cybersecurity360.it/legal/privacy-dati-personali/sistema-di-data-protection-la-documentazione-da-produrre-aggiornare-e-conservare/#post-46872-footnote-5); i.e. tutti i documenti cartacei ed informatici e in generale i records su ogni tipo di supporto idoneo a rendere evidente l’informazione (e.i. log file, audio, video ecc.).

**Documenti obbligatori e non obbligatori (ma raccomandati)**

Esaminiamo di seguito quale documentazione è auspicabile sia presente all’interno delle organizzazioni pubbliche e private, indicando da **chi** e **come** va prodotta, aggiornata e conservata e precisando che alcuni documenti sono prescritti come obbligatori dal GDPR mentre altri sono raccomandati come utili strumenti di governance del sistema.

**Il “Privacy Dashboard” e documenti connessi**

Si tratta di un documento non previsto dal GDPR e quindi non obbligatorio anche se per la sua utilità è fortemente raccomandato. Da molti è denominato “Manuale Privacy”, o **“Privacy Dashboard”,** un vero e proprio **strumento di controllo**, un **cruscotto operativo: s**i tratta di un brogliaccio, un documento sinottico che offre una vista completa di **“chi”** deve fare **“che cosa”** all’interno dell’organizzazione in materia di protezione dei dati personali.

Quindi, questo particolare documento dovrà riportare **l’organigramma privacy** con una descrizione generale dei compiti, ripartiti tra funzioni aziendali/aree organizzative omogenee e con l’indicazione **solo** dei manager/funzionari che le dirigono, ciascuno dei quali dovrà ricevere una designazione personale **scritta** che riporti i contenuti principali dei compiti loro attribuiti.

Costoro, nell’ambito della loro sfera di responsabilità, devono poi aver cura di predisporre, aggiornare e conservare dei **funzionigramma privacy**, i.e. dei documenti che indichino con precisione ruoli e responsabilità di tutte le entità cioè di tutte le persone fisiche che compongono le varie unità organizzative sottoposte al loro potere di direzione. Possono essere annessi al funzionigramma tutti gli atti di designazioni di incaricati/autorizzati da parte dell’esercente le funzioni di titolare e tutti i documenti relativi alla formazione degli stessi incaricati.

Si realizza così la c.d. **cascata dei compiti** (*waterfall model*) che rende facilmente dimostrabile la corretta attuazione del modello organizzativo prescritto dal GDPR e nel contempo attualizza il principio secondo il quale qualunque attività si svolga all’interno dell’organizzazione deve essere ricondotta alla sfera di responsabilità di una entità, cioè di una ben individuata persona fisica.

Continuando, all’interno del Privacy Dashboard*,* dopo l’organigramma va annotata tutta la documentazione necessaria a garantire un effettivo presidio dei dati che girano nei processi aziendali (quindi, documenti riguardanti la formazione, informative, moduli per l’esercizio dei diritti, piani, registro dei trattamenti, specifiche procedure ecc.).

Una precisazione importantissima: in corrispondenza di ogni documento annotato nel Privacy Dashboard va indicato il manager/funzionario, competente/responsabile a gestire l’attività documentata.

Esaminiamo ora di seguito in modo analitico la documentazione annotata sul Privacy Dashboard che deve essere coltivata da ciascun responsabile di funzione aziendale/area organizzativa omogenea.

**Documenti riguardanti la formazione**

Prima e più importante misura organizzativa è la formazione che crea consapevolezza e sensibilità diffuse e garantisce la tenuta del sistema. È specificamente prescritta sia dall’art. 29 che dall’art. 32 par. 4 del GDPR che, non a caso tratta la sicurezza del trattamento. Senza un’adeguata formazione del personale operante, qualsiasi misura tecnica od organizzativa è destinata a non avere efficacia.

La formazione è fondamentale nel senso letterale del termine: le attività di formazione sono le fondamenta del sistema di data protection.

Nel “Privacy Dashboard” dovrà essere indicata la persona fisica responsabile della formazione. Il DPO chiederà la massima attenzione e la massima cura per la formazione che deve essere fatta seriamente, deve cioè essere misurata e misurabile. Quindi al termine degli interventi formativi devono essere eseguiti dei test per verificare se e quanto il messaggio formativo è stato recepito.

Tutta la documentazione prodotta deve essere conservata dal citato responsabile della formazione.

**Documenti obbligatori**

**Informative e basi giuridiche**

Ogni trattamento di dati personali deve essere preceduto da una serie di informazioni che devono essere rese all’interessato per realizzare il principio di correttezza e trasparenza.

Per tale motivo, ogni responsabile di processo aziendale/procedimento amministrativo (c.d. **process owner**) ha l’onere di predisporre specifiche informative, attagliandole alle concrete attività di trattamento, avendo cura di inserire i contenuti minimi prescritti dagli artt. 13 e 14 GDPR. L’informativa deve contenere la descrizione del “ciclo di vita” dei dati e quindi anche gli eventuali destinatari o le eventuali categorie di destinatari, l’intenzione del titolare di trasferire i dati raccolti a un paese terzo o a un’organizzazione internazionale e l’esistenza o l’assenza di una decisione di adeguatezza della Commissione. In mancanza di una decisione di adeguatezza, vanno sempre specificate le garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. È fondamentale anche specificare sempre il periodo di conservazione dei dati oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

Nell’informativa vanno anche indicate le basi giuridiche che giustificano il trattamento. In particolare, se il trattamento si basa sul consenso o sul legittimo interesse è obbligatorio predisporre una ulteriore specifica documentazione.

Infatti, l’art.7, par.1 GDPR prescrive che qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l’interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Quindi il process owner dovrà disegnare una procedura per raccogliere il consenso e conservare in modo sicuro i relativi records.

Per basare il trattamento sul legittimo interesse, invece, lo stesso process owner farà bene a predisporre una specifica procedura per effettuare il c.d. “balacing test” ovvero un test comparativo tra il legittimo interesse del titolare e gli interessi o i diritti e le libertà fondamentali degli interessati. Molto utile al riguardo risulta essere la guida posta in **Allegato 1 al WP 217 – Parere 6/2014 del WP29** alla cui lettura si rinvia.

**Procedura e modulistica per l’esercizio dei diritti**

Il titolare del trattamento deve agevolare l’esercizio dei diritti degli interessati in materia di protezione dei dati personali e realizzare specifici adempimenti procedurali con i vincoli temporali fissati dall’art. 12 GDPR.

È pertanto necessario definire una procedura specifica, predisponendo contestualmente:

* designazioni/autorizzazioni scritte individuali per ogni entità chiamata ad applicare la procedura individuata;
* apposita modulistica.

**Documentazione relativa ai responsabili del trattamento**

L’art. 28 GDPR prescrive che:

* i trattamenti da parte di un responsabile del trattamento debbano essere disciplinati da un contratto o da altro atto giuridico che vincoli il responsabile stesso al titolare;
* il responsabile del trattamento metta a disposizione del titolare tutte le informazioni necessarie a garantire la compliance al GDPR e consenta allo stesso titolare di eseguire audit per verificare la corretta esecuzione delle istruzioni.

Pertanto in attuazione di tali disposizioni, la persona esercente le funzioni di titolare deve predisporre e conservare il contratto e tutti i documenti redatti nel corso del rapporto contrattuale con il responsabile.

**Registro dei trattamenti**

Il registro, prescritto dall’art. 30 GDPR, è un documento obbligatorio per i titolari e per i responsabili e uno dei più importanti strumenti di accountability, una preziosa risorsa di informazione per il Garante in fase di controllo. Peraltro, qualora il titolare non si doti di strumenti generali di governance del sistema, come il citato Privacy Dashboard, rimane un imprescindibile strumento di monitoraggio del titolare/responsabile.

Il registro deve riportare il censimento di tutti i trattamenti eseguiti. Può capitare che il responsabile non lo adotti quindi per sicurezza il titolare deve sempre pretendere che il responsabile gli trasmetta una copia.

La predisposizione e la gestione del registro è un compito attribuito all’esercente le funzioni di titolare il quale può anche delegare questa incombenza ad un manager/funzionario dell’organizzazione, avendo però la consapevolezza che la responsabilità rimane sempre ancorata alla sua sfera di competenze.

Il registro deve consentire di identificare i soggetti coinvolti nel trattamento dei dati, finalità, le categorie di interessati e dei dati trattati, chi accede agli stessi, a chi vengono comunicati, per quanto tempo sono conservati e quanto sono sicuri.

Seppure non previsti come obbligatori dal GDPR è opportuno inserire altri items che per ogni trattamento indichino le informative, le basi giuridiche ed il livello di rischio per i diritti e le libertà fondamentali degli interessati. Si ha così modo di evidenziare i trattamenti “a rischio elevato” sui quali andrà effettuata la [**valutazione di impatto (c.d. DPIA)**](https://www.cybersecurity360.it/legal/privacy-dati-personali/dpia-e-gdpr-che-ce-da-sapere-per-una-corretta-valutazione-dei-rischi-privacy/).

Va precisato che il registro non va inteso come una mera incombenza burocratica ma come un vero e proprio strumento operativo, analogo – per dare un’idea – ai registri obbligatori di magazzino delle medie e grandi aziende. Si comprende così anche il motivo per il quale il registro è funzionale all’esecuzione di audit interni e ad ispezioni da parte dell’Autorità di controllo.

**Documentazione riguardante le misure di sicurezza**

Le misure che garantiscono la sicurezza dei dati all’interno dell’organizzazione si dividono in due categorie: misure organizzative e misure tecniche. Queste ultime vanno individuate tenendo conto dello stato dell’arte e dei costi di attuazione, nonché della natura, dell’oggetto, del contesto e delle finalità del trattamento e considerando che l’art. 32 GDPR raccomanda, come misure tecniche minime la pseudonimizzazione e la cifratura dei dati.

Le preoccupazioni di dimostrabilità, in quest’area, concernono soprattutto le misure organizzative sia fisiche che logiche, volte ad assicurare su base permanente la riservatezza, l’integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento nonché a ripristinare tempestivamente la disponibilità e l’accesso dei dati personali in caso di incidente fisico o tecnico.

Per realizzare queste finalità *il responsabile della funzione IT* deve predisporre una **politica di sicurezza informatica** cioè l’insieme organico delle regole formali che definiscono le modalità di gestione degli strumenti informatici e dei dati dell’azienda o dell’ente in esame. Componenti della politica sono:

* l’autenticazione;
* l’integrità dei dati interna ed esterna;
* il backup dei dati;
* la sicurezza degli host;
* la sicurezza del network;
* la sicurezza fisica;
* la sicurezza delle operazioni;
* la gestione delle configurazioni (profilo di sicurezza minimo, c.d. “golden image”);
* meccanismi di alert attivati sui sistemi (SIEM et similia);
* le modalità operative di cambio della politica in caso di eventi esterni non previsti.

Per applicare la politica di sicurezza sulle entità, ogni Process Owner, sulla base di una specifica delega rilasciata dall’esercente le funzioni di titolare, sistematicamente annotata sul Privacy Dashboard, dovrà effettuare **designazioni personali**, in forma scritta.

Tali designazioni, in linea con le indicazioni offerte dal § 12.1 della prassi di riferimento UNI PdR 43.1:2018, devono riprendere i contenuti principali dei singoli compiti attribuiti a ciascun collaboratore.

Esse dovrebbero disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell’art. 28 GDPR, ovvero che il designato/autorizzato sia in possesso e fornisca garanzie sufficienti su: natura, finalità, durata e modalità del trattamento.

Il Process Owner dovrebbe somministrare e verificare gli atti di designazione all’inizio delle attività e periodicamente, almeno una volta l’anno, le designazioni sono oggetto di un processo di analisi ed eventuale revisione.

Se nell’organizzazione è presente un **amministratore di sistema** cioè un professionista dedicato alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, è necessario applicare quanto disposto dal Garante, con provvedimento del 27 novembre 2008, tuttora applicabile. Quindi:

* l’amministratore di sistema dovrà essere **designato con atto scritto individuale** che rechi l’elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
* gli **estremi identificativi** delle persone fisiche designate amministratori di sistema, con **l’elenco delle funzioni ad essi attribuite,** devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti da parte del Garante;
* qualora l’attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, **i titolari pubblici e privati** sono tenuti a rendere nota o conoscibile l’identità degli amministratori di sistema nell’ambito delle proprie organizzazioni, secondo le caratteristiche dell´azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti. Ciò, avvalendosi dell’informativa resa agli interessati ai sensi dell’art. 13 GDPR e dell’art.4. comma 3 dello Statuto dei Lavoratori.

Dopo aver implementato le misure di sicurezza organizzative, in attuazione di quanto prescritto dall’art.32, par.1, lettera d) GDPR, l’esercente le funzioni di titolare o un suo idoneo delegato deve predisporre una procedura per testare, verificare e valutare regolarmente l’efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Si tratta del noto [**penetration test (o pen-test)**](https://www.cybersecurity360.it/soluzioni-aziendali/penetration-test-cose-come-funziona-e-a-che-serve/) eseguito dai **White hat hackers** funzionale ad analizzare e valutare la robustezza di un sistema informatico.

**Documentazione delle valutazioni di impatto (DPIA)**

Mentre, come si è visto, le valutazioni di sicurezza devono essere eseguite su tutti i trattamenti, le valutazioni di impatto vanno effettuate solo quando il trattamento prevede l’uso di nuove tecnologie e può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

L’articolo 35 del GDPR indica i criteri in base ai quali si individuano i casi nei quali la DPIA è necessaria e il provvedimento del GPDP n. 467 dell’11/10/2018 pone analiticamente l’elenco delle tipologie di trattamenti da sottoporre a valutazione di impatto.

Quindi l’esercente o un idoneo delegato, specificamente indicato sul Privacy Dashboard dovrà eseguire e documentare il processo sviluppato seguendo precisamente **le Linee Guida WP 248 rev.01 adottate dal WP29 il 4 ottobre 2017**.

**Documenti concernenti la gestione di eventuali data breach**

Le misure di sicurezza sopra descritte per quanto accurate possano essere, non potranno mai annullare la probabilità che si verifichi un [**data breach**](https://www.cybersecurity360.it/legal/data-breach-le-procedure-corrette-per-gestire-la-crisi/) cioè una violazione di sicurezza.

Quali sono gli oneri di documentazione in questo caso?

Quando si verifica un data breach il titolare deve:

* notificare entro 72 ore al Garante ai sensi dell’art. 33 la violazione, solo se questa presenta un rischio per i diritti e le libertà delle persone fisiche;
* comunicare agli interessati la violazione, quando questa è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
* documentare qualsiasi violazione dei dati personali (anche quelle non notificate al Garante e non comunicate agli interessati) comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Pertanto il titolare ha l’obbligo di tenere un registro delle violazioni di sicurezza da mantenere aggiornato.

Inoltre, poiché è necessario reagire al data breach in modo tempestivo, strutturato ed efficace appare opportuno predisporre una procedura di gestione della violazione individuando le entità coinvolte nel particolare processo ed affidando loro appositi compiti per iscritto.

**Documentazione dei flussi di comunicazione: con il DPO, a terzi e fuori dal SEE**

Il titolare del trattamento deve assicurarsi che il DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali[[10]](https://www.cybersecurity360.it/legal/privacy-dati-personali/sistema-di-data-protection-la-documentazione-da-produrre-aggiornare-e-conservare/#post-46872-footnote-10), al fine di consentirgli lo svolgimento dei compiti di consulenza nei confronti del titolare medesimo, oltre che di sorveglianza sulla conformità dei trattamenti, che gli sono attribuiti dal GDPR.

Quindi devono essere adeguatamente documentati:

* tutti gli atti connessi alla designazione del DPO;
* tutti i flussi di comunicazione con il DPO.

È importante precisare che il titolare, nei casi in cui decida di non seguire le indicazioni offerte dal DPO, deve redigere e conservare un documento nel quale indichi i motivi per i quali ha inteso assumere la decisione difforme dalle indicazioni e dai suggerimenti ricevuti.

La comunicazione dei dati a terzi e l’esportazione dei dati al di fuori dello SEE vanno adeguatamente documentate, magari anche strutturando specifiche procedure nelle quali vengano specificati i presupposti, i contesti e le modalità di effettuazione delle comunicazioni a terzi e dell’esportazione di dati personali. Come si è detto, questo tipo di documentazione deve trovare riscontro nelle informative rese agli interessati ai sensi degli artt. 13 e 14 GDPR.

Tutti gli adempimenti finora descritti costituiscono un arduo onere organizzativo che però è bene adempiere per proteggere in concreto i diritti e le libertà fondamentali delle persone fisiche e per creare il clima di fiducia necessario per la libera circolazione dei dati personali ed il connesso sviluppo dell’economia 4.0.

Ma se questi alti obiettivi non costituiscono per i titolari sufficienti fattori di motivazione, si consideri la probabilità di pesanti e dissuasive sanzioni in caso di inadempimento.

Valga come monito la sanzione pecuniaria di 300.000 euro che all’inizio del 2021 il Garante ha irrogato ad un importante Ente pubblico perché, tra l’altro, dopo l’ispezione, quanto dichiarato dallo stesso Ente nelle note di controdeduzione “non è stato supportato da un’adeguata documentazione atta a comprovare quali livelli decisionali erano stati coinvolti, le valutazioni effettuate, le ragioni sottese alle decisioni prese e le misure adottate in relazione al trattamento dei dati personali (si pensi agli aspetti sulla valutazione del rischio o alla valutazione di impatto sulla protezione dei dati).

Peraltro, non è nemmeno emerso un adeguato coinvolgimento, da parte del titolare del trattamento, del ruolo del DPO, considerato che invece, sulla base del Regolamento, quest’ultimo avrebbe dovuto essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali”.