MAST
SOLUTION TECHNOLOGY

WhatsApp
3356694060

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

GDPR "il giorno dopo": ACCOUNTABILITY

consigli per titolari e responsabili

Il principio di **accountability** previsto dal GDPR implica non solo la piena "responsabilizzazione" **di titolari e responsabili del trattamento** nella predisposizione di idonee misure tecniche e organizzative a protezione dei dati, ma piuttosto prevede **la dimostrazione, il dar di conto con evidenze concrete, oggettive e misurabili della corretta applicazione degli adeguamenti** imposti dal Regolamento UE 2016/679.

Occorre quindi documentare e giustificare tutto?

Molti criticano il GDPR perché, pur ponendosi sostanzialista e meno formale, nasconde con l'accountability una burocrazia persino "potenziata"; ed ovviamente, in molti hanno fatto ricorso a documenti fiume, "nomine" spesso non circostanziate e con lunghissime clausole inapplicabili e fuori contesto, voluminose procedure consegnate al personale e altro ancora.

Invece, la dimostrazione di prassi corrette **non è affatto sinonimo di tonnellate e tonnellate di carta**.

È ovvio, però, che governare i processi implica necessariamente la produzione di una certa quantità di documentazione, in formato cartaceo e/o elettronico. Che deve essere **essenziale, chiara e pertinente con le necessità di fornire le evidenze di quanto svolto**.

Come dimostrare, dunque, la corretta applicazione delle misure tecniche e organizzative che vengono poste in essere dal titolare o dal responsabile?

Ovviamente **non esistono**, né potrebbero esistere, **regole universali** per tutte le organizzazioni; tuttavia, possiamo provare a identificare delle modalità di verifica per alcune iniziative che ogni organizzazione dovrebbe già aver intrapreso:

WhatsApp
3356694060

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Sensibilizzazione e formazione del personale

È stato già detto e ripetuto più volte quanto sia importante la consapevolezza del personale, e più in generale di tutti coloro che sono addetti alle attività di trattamento.

La dimostrazione di un'idonea preparazione di certo non si misura soltanto sulla lettera di autorizzazione o sullo stile del documento di istruzioni; in caso di audit o controllo, il verificatore con ogni probabilità potrebbe coinvolgere degli operatori e chiedere di eseguire certe operazioni correlate al trattamento analizzato, anche con domande specifiche e dirette; l'Autorità e il Nucleo Privacy della Guardia di Finanza in particolare, pur attenti a non intimorire eccessivamente gli interlocutori, cercano spesso di comprendere se il personale coinvolto è consapevole dei trattamenti che sta effettuando, e se ad esempio abbia chiaro il ruolo della propria organizzazione per quel trattamento (titolare o responsabile).

Ecco perché ad un corso di "alfabetizzazione" al GDPR, va sempre affiancata **formazione specifica**, e azioni ulteriori quali "esercitazioni di gruppo" o **simulazioni**, anche informali e in forma di serious games.

Anche l'aver coinvolto le persone nella preparazione del registro delle attività di trattamento, nelle informative e nelle procedure, contribuisce alla creazione della cultura della protezione dati in azienda.

Quando il "modello privacy" viene preparato da una sola funzione aziendale con l'ausilio di super consulenti, e poi viene "imposto" come una scure che si abbatte sull'organizzazione, la consapevolezza può venir meno.

Questo semplice elenco di regole potrebbe aiutare:

1. **insegnare a mettere al centro i trattamenti**, non gli adempimenti; far provare gli autorizzati a ripensare i trattamenti svolti nell'ottica del rischio, chiedendo di ipotizzare possibili conseguenze per gli interessati (sviluppa l'approccio risk-based di tipo attivo);
2. **condividere l'evoluzione della framework che si vuole impostare**, coinvolgere quanti più attori possibili nella mappatura delle attività di trattamento;
3. **rendere pubblici al personale i registri delle attività di trattamento**, e se possibile l'elenco dei soggetti autorizzati con il riferimento ai trattamenti autorizzati; non si deve aver paura di rendere noto alle unità organizzative il modo di lavorare, e gli eventuali fornitori, di altre funzioni aziendali; il "divide et impera" con la compliance non si addice;
4. **aumentare senza timore il grado di conoscenza tecnologico del personale**, spiegando e non imponendo le misure tecniche, anche se l'uso di nuovi strumenti, o metodologie di crittografia e/o pseudonimizzazione possono inizialmente "spaventare", lo sforzo di elevare il livello e gli skills degli operatori è un elemento di grande importanza.

È ovvio che tali azioni prevedono un percorso di adeguamento più lento, ma sicuramente l'efficacia e la metabolizzazione della logica della protezione dati non è comparabile con quella che si può ottenere mediante l'imposizione del rispetto sterile di regole e procedure.

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Registrazione delle operazioni per produrre evidenze

Dobbiamo comunque produrre evidenze, quindi le azioni, anche formative, vanno verbalizzate. E non solo.

Facciamo dunque **qualche ulteriore esempio di rendicontazione necessaria**. Sappiamo che è bene documentare il perché, per una certa attività di trattamento, si debbano utilizzare anche categorie particolari di dati personali; oppure, per un'altra attività di trattamento, potremmo dover giustificare il legittimo interesse quale base giuridica.

Bene, quale miglior modo del registro delle attività di trattamento per documentare tali presupposti? Rispetto alle informazioni obbligatorie previste dall'Art. 30, possiamo tranquillamente aggiungere le informazioni necessarie.

È importante sottolineare che, più in generale, registrare le operazioni, anche mediante semplici fogli elettronici (se non si dispone di un software per la gestione della compliance o di log informatizzati prodotti da sistemi di controllo), sono **un ottimo modo per rendicontare il governo dei processi**.

Ecco, oltre ai registri delle attività di trattamento, una lista di esempio di alcuni registri di operazioni che possiamo adottare, la cui tenuta è snella ed efficace (ancor più se informatizzata con un software, ovviamente) e al tempo stesso utile per la rendicontazione:

- **elenco dei soggetti autorizzati alle attività di trattamento**, per tenere sotto controllo sia le persone autorizzate sotto la diretta autorità, sia i responsabili del trattamento; per ogni soggetto, si può tenere traccia delle seguenti informazioni:

1. ambiti di trattamento autorizzati;
2. data inizio incarico/autorizzazione al trattamento;
3. data fine incarico/autorizzazione al trattamento;
4. data prossima revisione autorizzazioni;
5. data documento di istruzioni impartite;
6. data erogazione formazione;
7. data ultima verifica di conformità;
8. modalità esecuzione verifica (es. questionario due diligence, audit fisico, etc.);
9. esito verifica;
10. rilievi verifica;
11. data effettuazione prossima verifica.

- **registro censimento e aggiornamento sistemi/server/postazioni/mobile devices;**
- **registro riutilizzo/distruzione dispositivi e supporti elettronici;**
- **registro backup e prove di ripristino;**
- **registro esercizio dei diritti degli interessati;**
- **registro relazioni con l'autorità garante**;
- **registro incidenti di sicurezza informazioni;**
- **registro dei data breach.**

Sono soltanto alcuni esempi, ma possono essere uno spunto per spiegare che il documentare in modo sostanziale può essere realizzabile anche registrando in modo semplice e applicando procedure snelle

WhatsApp
3356694060

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Procedure e istruzioni a responsabili e autorizzati

L'attuazione del governo dei processi e l'inserimento costante della valutazione dei rischi sin dalla progettazione, presuppone che titolari e responsabili del trattamento, anche al fine di mitigare il livello di rischio abbattendo la probabilità di errore da parte degli operatori per inconsapevolezza o superficialità, adottino **tecniche volte ad assicurare la piena comprensione delle istruzioni e procedure impartite**.

Nella logica di **accountability** non è sufficiente, dunque, conservare la copia controfirmata di un documento fra le parti contenente le istruzioni. Fra le evidenze da predisporre per la **verifica dell'efficacia**, dovrebbero essere presenti, dunque:

- questionari di verifica della comprensione delle istruzioni impartite (realizzabili anche mediante l'utilizzo dell'e-learning, o mediante strumenti di surveys online);
- rapporti di audit su case studies specifici, quali "prove pratiche" o esercitazioni e simulazioni.

Tali evidenze verranno ben presto richieste sempre più spesso anche nei rapporti fra titolari e responsabili del trattamento per documentare garanzie di affidabilità richieste.

Ad esempio, è ovvio che nessun titolare o responsabile del trattamento si può permettere di non aver verificato che il personale che opera sotto la sua diretta autorità abbia letto e compreso, e sappia anche applicare, le istruzioni contenute nella procedura per la gestione dei data breach (che ovviamente deve essere tarata per una facile comprensione, e appunto della quale va sicuramente verificata la conoscenza).

WhatsApp
3356694060

MAST di Walter Solati
Via Pertini 9 - 20090 Settala (MI)
Cod.Fis.: SLTWTR65P27F205Z
P.Iva 09210860962 - REA MI 2075970
info@mast.technology - Tel +39 02.95307344

Verifiche tecnologiche di sistemi e applicazioni

L'aspetto di **ICT governance** è forse il più complesso e oneroso, ma al tempo stesso importantissimo per la protezione delle infrastrutture e degli strumenti tecnologici, perché è quello che sicuramente prevede la più ampia gamma di verifiche, controlli, soluzioni e strumenti.

In questo campo, tuttavia, l'utilizzo delle norme standard e di framework di sicurezza consolidati consente, attraverso **una ragionata selezione dei controlli in base al contesto**, di ottenere in modo a volte quasi "naturale" una lista di misure idonee da adottare e punti di verifica e di riesame da includere nella valutazione continua dei rischi per la gestione dei processi.

Ed oltre al GDPR, come ben sappiamo, anche altre normative (ad esempio, NIS per gli Operatori di Servizi Essenziali, le misure minime di sicurezza AGID per la PA ecc.) prevedono per titolari e responsabili l'implementazione di sistemi di gestione per la sicurezza e l'attribuzione di ruoli e responsabilità specifiche.

È questo lo scenario dove si giocherà la credibilità degli operatori sul campo e dove alcuni investimenti significativi (ad esempio, per vulnerability assessment e penetration test) potranno contribuire non solo a rendicontare la necessaria attenzione ai propri meccanismi di protezione, ma anche a evidenziare anomalie e falle nei propri sistemi, rivalutare i rischi e migliorare la governance ICT, elemento essenziale per ogni impresa o amministrazione.