Audit ai sensi del Regolamento Europeo 2016/679: Un Format Metodologico

PREMESSA

Con la recente entrata in vigore, lo scorso 25 maggio 2018, del Regolamento sulla Protezione dei Dati Personali, l' Europa prende finalmente atto di un cambiamento epocale: la nostra società ultratecnologica, iperconnessa, si muove ormai in un cyberspazio dai confini sfumati, difficilmente individualizzabili in cui non è raro che gli attori (civili ed economici) perdano *il controllo* dei propri dati personali.
Per mantenere la competitività sui mercati internazionali, trainata dalla fiducia dei consumatori, la Commissione emette il Regolamento, profondamente innovativo, la cui estrema ratio vede la sinergia inscindibile della protezione del dato personale sotto un duplice profilo:

- il primo afferisce alla dimensione della *safety* del trattamento, l'aspetto normativo/documentale, finalizzato a garantire che il flusso sui dati non leda i diritti fondamentale dell'interessato.
- il secondo afferisce alla dimensione della *security* del trattamento, l'aspetto tecnologico/organizzativo, che mira a garantire la confidenzialità, l'integrità e la disponibilità del dato personale, nel passaggio attraverso l'infrastruttura operativa.

Il Regolamento cambia profondamente la logica degli audit relativi alla normativa privacy: non esistono più misure *minime* di sicurezza da implementare ma viene introdotto un moderno approccio *risk based,* in base al quale il titolare del trattamento si impegna a mettere in campo tutte le misure ritenute *adeguate* al rischio stimato.

Questa sostanziale "rivoluzione copernicana" impatta notevolmente sulle procedure operative consulenziali: non basta più controllare la sussistenza di un elenco di requisiti (quello che era l'allegato B del Codice della Privacy); si tratta invece di effettuare una seria e competente analisi del rischio preliminare e, qualora si individui un trattamento ad alto impatto, procedere con la dpia (Data Protection Impact Assessment).

Il presente lavoro nasce da un'istanza prima di tutto operativa.
Gli addetti ai lavori sentono fortemente la necessità di un format metodologico che fornisca delle linee guida attraverso cui plasmare l'attività di audit e che dia una risposta riproducibile e intersoggettiva alla domanda sulla necessità o meno di procedere alla valutazione di impatto.

L'approccio presentato nel presente lavoro consiste in un modello applicabile, dai *tecnici*[1] del settore, a tutte le realtà, anche le più piccole, che intendano richiedere un audit esaustivo ai sensi del GDPR che analizzi contestualmente le due grandi aree operative, inscindibili in vista della conformità, del *privacy audit* e del *security audit*.

La metodologia di analisi del rischio alle proprietà CIA delle informazioni (riservatezza, inte-

1 Riteniamo auspicabile che la compilazione del registro e soprattutto l'analisi del rischio sia condotta da tecnici del settore, Avvocati esperti di informatica giuridica, Analisti Informatici, Managers della Sicurezza Informatica

grità, disponibilità), presentata in questo lavoro, attraversa entrambi gli audit trasversalmente.

Essa consiste nell'attribuzione di un punteggio all'asset informativo, alla probabilità di occorrenza della minaccia (motivando il tutto con riferimenti al Rapporto Clusit o a riviste del settore in modo che l'analisi sia almeno riproducibile), ponderato sul livello di "vulnerabilità" della struttura che si evince dal check dei controlli di sicurezza.

Ne esce fuori un punteggio che, se maggiore di un certo valore (usando una certa matrice del rischio = 36 ad esempio), fa scattare l'alert per la dpia.

A valle della procedura viene inoltre proposto un questionario sulle *best practices di sicurezza* da somministrare al personale che accede alle postazioni informatiche.
Troppo spesso infatti, nonostante un impeccabile impianto documentale e l'implementazione di sistemi informativi tecnicamente adeguati, proprio la risorsa umana risulta essere l'anello debole della catena[2].
E' importante quindi formare il personale ai concetti basilari della sicurezza informatica e introdurre questa dimensione come una variabile strategica all'interno dell'organizzazione.

LA METODOLOGIA

Il modello proposto nel presente lavoro consiste in una serie di schede excel finalizzate a far emergere le caratteristiche salienti del trattamento dei dati personali effettuato da un Titolare e il conseguente impatto sui diritti e le libertà degli interessati.
La navigazione tra le schede può avvenire attraverso il menù in basso mostrato in FIGURA 1.

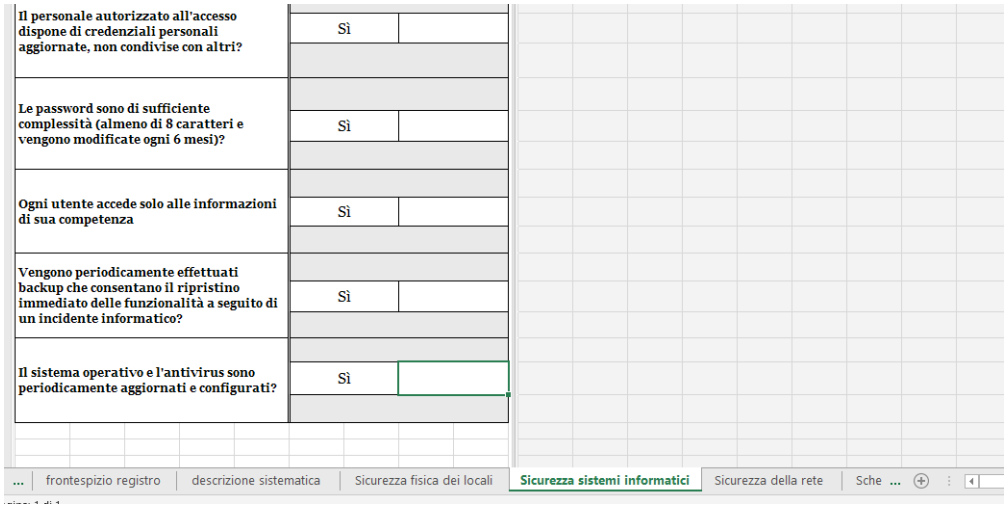


FIGURA 1

Il primo tab, "istruzioni" fornisce una prima overview su ciò che si andrà a realizzare (FIGURA 2):

- una FASE PRELIMINARE di identificazione dei trattamenti, supportata da interviste mirate al titolare e ai referenti di ogni settore operativo
- il PRIVACY AUDIT, una descrizione sistematica e accurata del trattamento sotto l'aspetto della

2 Gli attacchi di Social Engineering, che sfruttano le debolezze umane per violare un sistema informatico ultraprotetto sono sempre più diffusi.

conformità sostanziale e documentale ai principi sanciti dal GDPR;

- il SECURITY AUDIT, una serie di controlli sulla piattaforma operativa, la sicurezza fisica dei locali, la sicurezza delle postazioni informatiche, la sicurezza della rete, la conformità del sito web (considerato come ulteriore *entry point* dal quale i dati personali possono fluire all'interno della struttura censita).

Dalla valutazione congiunta dei due audit consegue l'*attribuzione di un punteggio*, opportunamente motivato dal professionista, che "fotografa" lo stato dell'arte dell'audit appena finalizzato:

- **3** = controllo sotto la media
- **2** = controllo nella media
- **1** = controllo sopra la media

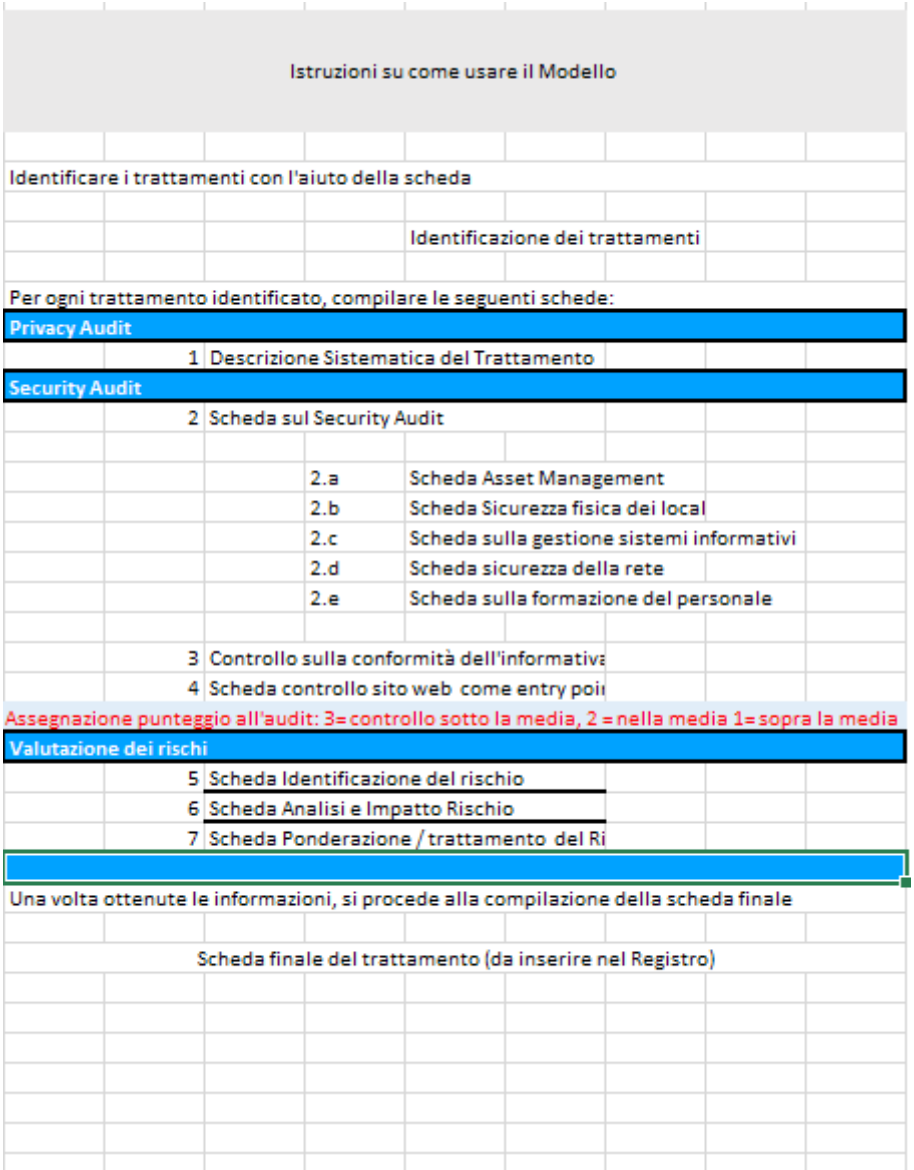


FIGURA 2

Tale valore servirà a valle del processo di valutazione del rischio per "ponderare" l'equazione del rischio intrinseco del trattamento con il livello di vulnerabilità (intesa come mancanza di controlli) emergente dall'audit.

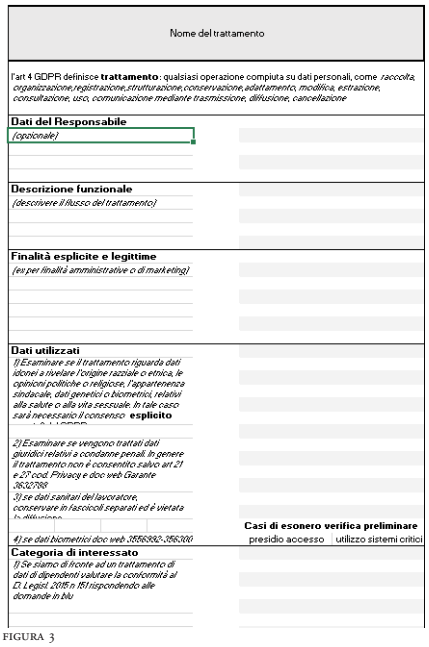
- il processo di RISK ASSESSMENT**:**
  1. inventario degli asset;
  2. determinazione dell'impatto dell'asset lungo le tre dimensioni della confidenzialità, integrità e disponibilità;
  3. identificazione delle minacce applicabili al contesto sotto indagine;
  4. determinazione (motivata) della probabilità di occorrenza della minaccia;
  5. calcolo della matrice del *rischio intrinseco;*
  6. calcolo del livello di *rischio totale* del trattamento;
  7. ponderazione del rischio, vale a dire la valutazione di accettabilità o di pianificazione di misure correttive (la valutazione di impatto con relativo trattamento è auspicabile se il rischio totale è maggiore di 36);

- la metodologia si conclude con una SCHEDA FINALE che riepiloga la descrizione sistematica del trattamento, il risultato dell'analisi del rischio e integra un sistema di gestione delle segnalazioni delle violazioni rilevate al Garante, unitamente alle misure intraprese per limitarne l'impatto.

Una volta identificato il trattamento, se necessario con l'aiuto dell'elenco (non esaustivo) contenuto nel tab "identificazione del trattamento", si entra nel cuore del processo di audit.

IL PRIVACY AUDIT

La scheda "descrizione sistematica" (FIGURA 3) è finalizzata ad individuare le caratteristiche salienti del trattamento ai sensi della conformità ai principi del GDPR. Qualora esista un *Responsabile della Protezione dei Dati* viene subito individuato in quanto una costruttiva collaborazione con lui incrementerebbe in maniera rilevante il livello di efficacia dell'audit.


Nome del trattamento

l'art 4 GDPR definisce **trattamento**: qualsiasi operazione compiuta su dati personali, come *raccolta, organizzazione, registrazione, strutturazione, conservazione, adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, cancellazione*

Dati del Responsabile

(opzionale)

Descrizione funzionale

(descrivere il flusso del trattamento)

Finalità esplicite e legittime

(es per finalità amministrative o di marketing)

Dati utilizzati

1) Esaminare se il trattamento riguarda dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche o religiose, l'appartenenza sindacale, dati genetici o biometrici, relativi alla salute o alla vita sessuale. In tale caso sarà necessario il consenso **esplicito**

2) Esaminare se vengono trattati dati giuridici relativi a condanne penali. In genere il trattamento non è consentito, salvo art 21 e 27 Cod. Privacy e doc web Garante 3632788

3) se dati sanitari del lavoratore, conservare in fascicoli separati ed è vietata

Casi di esonero verifica preliminare

presidio accesso | utilizzo sistemi critici

4) se dati biometrici doc web 2556982-2562300

Categoria di interessato

1) Se siamo di fronte ad un trattamento di dati di dipendenti valutare la conformità al D. Legisl. 2015 n.151 rispondendo alle domande in blu

FIGURA 3

Nome del trattamento

l'art 4 GDPR definisce **trattamento**: qualsiasi operazione compiuta su dati personali, come *raccolta, organizzazione, registrazione, strutturazione, conservazione, adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, cancellazione*

Dati del Responsabile

(opzionale)

Descrizione funzionale

(descrivere il flusso del trattamento)

Finalità esplicite e legittime

(es per finalità amministrative o di marketing)

Dati utilizzati

1) Esaminare se il trattamento riguarda dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche o religiose, l'appartenenza sindacale, dati genetici o biometrici, relativi alla salute o alla vita sessuale. In tale caso sarà necessario il consenso **esplicito**

2) Esaminare se vengono trattati dati giuridici relativi a condanne penali. In genere il trattamento non è consentito, salvo art 21 e 27 Cod. Privacy e doc web Garante 3632788

3) se dati sanitari del lavoratore, conservare in fascicoli separati ed è vietata

Casi di esonero verifica preliminare

presidio accesso | utilizzo sistemi critici

4) se dati biometrici doc web 2556982-2562300

Categoria di interessato

1) Se siamo di fronte ad un trattamento di dati di dipendenti valutare la conformità al D. Legisl. 2015 n.151 rispondendo alle domande in blu

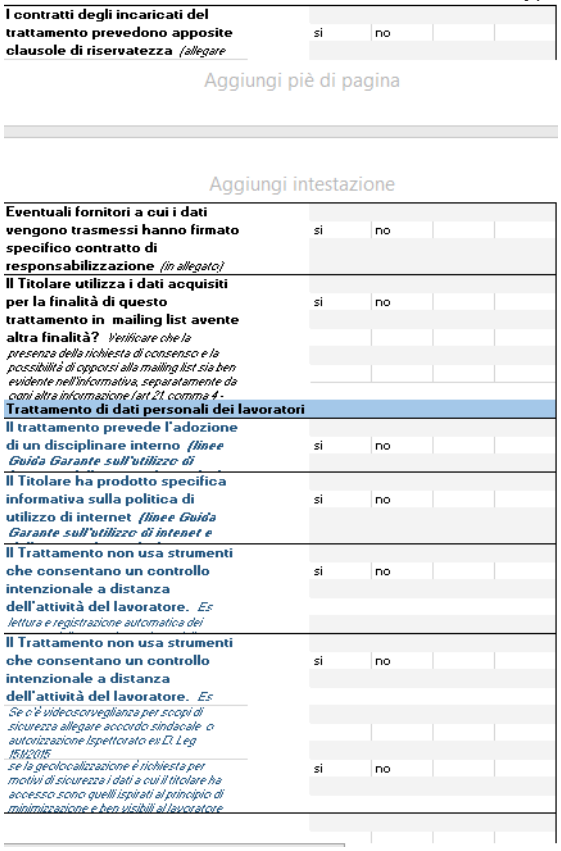
Segue il campo "*descrizione funzionale*" nel quale viene descritto il flusso operativo del trattamento.

Successivamente si verifica l'esistenza di *finalità esplicite e legittime*[3], l'eventuale presenza di *dati particolari* ex art. 9, per i quali vada richiesto il consenso esplicito, dati biometrici, giudiziari ecc.

I principi di necessità, pertinenza e minimizzazione sanciti dal Regolamento richiedono che i dati richiesti per un determinato trattamento siano strettamente quelli che servano per una certa finalità. Acquisendo queste informazioni il consulente saprà già formarsi un' idea sulla conformità ai suddetti principi.

3 Come richiesto dal Regolamento Europeo è *la finalità che fa il trattamento*. A questo punto è necessario che il consulente presti attenzione all'eventualità di trovare un trattamento avente più finalità. Con riferimento al principio di trasparenza, solo in presenza di opportune condizioni (ad esempio la presa d'atto che il flusso operativo sia il medesimo o che le finalità siano correlate) è possibile mantenere l'accorpamento: nel caso di finalità di marketing ad esempio è suggerita un'informativa separata.

Nel caso in cui il trattamento dati riguardi i *dipendenti*, viene richiesta la conformità al decreto legislativo 151/2015 circa l'eventuale sussistenza di controllo a distanza intenzionale (FIGURA 4).



I contratti degli incaricati del trattamento prevedono apposite clausole di riservatezza *(allegare*	si	no
Aggiungi piè di pagina		
Aggiungi intestazione		
Eventuali fornitori a cui i dati vengono trasmessi hanno firmato specifico contratto di responsabilizzazione *(in allegato)*	si	no
Il Titolare utilizza i dati acquisiti per la finalità di questo trattamento in mailing list avente altra finalità? *Verificare che la presenza della richiesta di consenso e la possibilità di opporsi alla mailing list sia ben evidente nell'informativa, separatamente da ogni altra informazione (art 21, comma 4 -*	si	no
Trattamento di dati personali dei lavoratori		
Il trattamento prevede l'adozione di un disciplinare interno *(linee Guida Garante sull'utilizzo di*	si	no
Il Titolare ha prodotto specifica informativa sulla politica di utilizzo di internet *(linee Guida Garante sull'utilizzo di intenet e*	si	no
Il Trattamento non usa strumenti che consentano un controllo intenzionale a distanza dell'attività del lavoratore. *Es lettura e registrazione automatica dei*	si	no
Il Trattamento non usa strumenti che consentano un controllo intenzionale a distanza dell'attività del lavoratore. *Es Se c'è videosorveglianza per scopi di sicurezza allegare accordo sindacale o autorizzazione Ispettorato ex D. Leg 151/2015*	si	no
se la geolocalizzazione è richiesta per motivi di sicurezza i dati a cui il titolare ha accesso sono quelli ispirati al principio di minimizzazione e ben visibili al lavoratore	si	no

FIGURA 4

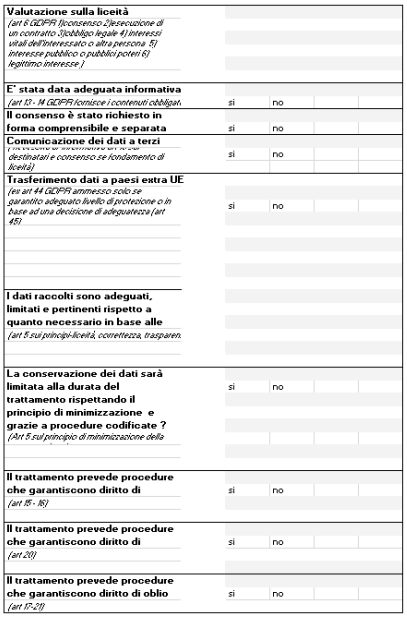
Il check successivo riguarda la *durata* del trattamento. Il mantenimento del dato infatti, sempre per il principio di minimizzazione, non può essere indiscriminato; il periodo di conservazione deve essere contenuto ed esaurirsi con l'esaurirsi della finalità.

Nei campi successivi viene richiesta la "fotografia" delle risorse utilizzate nel flusso operativo del trattamento: qualora vengano utilizzate risorse esterne (collaboratori, consulenti, professionisti ai diversi livelli della struttura organizzativa) diventa necessario popolare un *organigramma* della privacy, mappare il passaggio del dato all'esterno e nominare il soggetto affidatario Responsabile del trattamento ai sensi dell'art. 28. Ciò comporta il trasferimento del centro di imputazione della responsabilità del trattamento dal titolare al Responsabile nominato, il quale viene chiamato al rispetto dei principi del Regolamento, delle finalità e dei mezzi stabiliti dal titolare e delle misure di sicurezza *adeguate* ai sensi dell'art. 32.

Segue l'identificazione delle risorse hardware (computer, server, firewall, router, dispositivi di sicurezza) e software (programmi utilizzati, gestionali, web service di posta[4] ecc) allo scopo di controllare lo stato di sicurezza e l'avvenuto aggiornamento dell'infrastruttura tecnologico-operativa.

Per ogni trattamento inoltre, andranno individuati gli incaricati alle mansioni elaborative sui dati. Essi dovranno essere mappati nell'organigramma, formati opportunamente dal titolare e nominati *persone autorizzate al trattamento* con un atto scritto che stabilisca, con clausole precise, le istruzioni ad un uso conforme dei dati personali.

Sempre con riferimento alle risorse umane, un audit approfondito non trascende da una verifica sull'esistenza, da un lato, nel contratto di lavoro, di opportune clausole di riservatezza che vincolino il lavoratore anche oltre la fine della prestazione concordata, dall'altro di procedure aziendali chiare che non lascino margine discrezionale agli operatori in caso di incidente o di gestione delle crisi.



Valutazione sulla liceità *(art 6 GDPR [consenso 2]esecuzione di un contratto 3]obbligo legale 4] interessi vitali dell'interessato o altra persona 5] interesse pubblico o pubblici poteri 6] legittimo interesse)*		
E' stata data adeguata informativa *(art 13 - Il GDPR fornisce i contenuti obbligat.*	si	no
Il consenso è stato richiesto in forma comprensibile e separata	si	no
Comunicazione dei dati a terzi *destinatari e consenso se fondamento di liceità)*	si	no
Trasferimento dati a paesi extra UE *(ex art 44 GDPR ammesso solo se garantito adeguato livello di protezione o in base ad una decisione di adeguatezza (art 45)*	si	no
I dati raccolti sono adeguati, limitati e pertinenti rispetto a quanto necessario in base alle *(art 5 sul principio liceità, correttezza, trasparen.*		
La conservazione dei dati sarà limitata alla durata del trattamento rispettando il principio di minimizzazione e grazie a procedure codificate ? *(Art 5 sul principio di minimizzazione della*	si	no
Il trattamento prevede procedure che garantiscono diritto di *(art 15 - 16)*	si	no
Il trattamento prevede procedure che garantiscono diritto di *(art 20)*	si	no
Il trattamento prevede procedure che garantiscono diritto di oblio *(art 17-21)*	si	no

FIGURA 5

4 Qualora il Titolare conservi dati personali nei server di providers di posta elettronica è necessario richiedere l'addendum con cui detti gestori si autonominano *data processor*. Se dovesse avvenire una violazione dei loro datacenter infatti, per il modello di responsabilità condivisa essi risponderebbero per la sicurezza fisica degli asset.

I controlli seguenti entrano nel vivo del privacy audit, indagando il *fondamento di liceità (*figura *5),* la presenza di adeguata informativa, ai sensi degli artt 13 e 14, la presenza del *consenso* documentabile, se necessario, l'eventuale comunicazione dei dati a terzi o in paesi extra UE (per i quali sia necessario verificare la decisione di adeguatezza della Commissione) e la sussistenza di procedure per garantire agli interessati l'*esercizio dei diritti* di accesso, di modifica, di limitazione, di opposizione e, novità rispetto al vecchio Codice della Privacy, *del diritto all'oblio* e alla *portabilità*.
A completare il privacy audit, una scheda supplementare di controllo sul contenuto minimo dell'informativa.

IL SECURITY AUDIT

Abbiamo visto che il trattamento del dato avviene *attraverso* una piattaforma elaborativa. Lo scopo del security audit è di identificare gli asset strategici che ne fanno parte, e di verificare la presenza di alcuni requisiti essenziali che ne garantiscano la sicurezza.
Ogni asset viene valutato (figura 6) sulla base dell'impatto che potrebbe generare sui diritti e le libertà degli interessati qualora venisse meno ognuna delle 3 proprietà CIA dell'informazione che intende veicolare (figura 6).

Security Audit - scheda introduttiva				
Il check preliminare ha l'obiettivo di fotografare lo stato attuale della struttura sotto il profilo della sicurezza dei dati trattati. I controlli di sicurezza si ispirano a quelli consigliati dal framework nazionale NIST. Compilare tante schede quanti sono gli asset informativi da valutare				
Dati dell'Auditor				
Asset da proteggere				
(Informazione-processo-prodotto)				
Valore attribuito	a_ris	a_int	a_disp	
parametri: assegnare un valore da 0 a 3 all'informazione, a secondo dell'impatto che si avrebbe sui diritti dell'interessato se venisse meno la riservatezza, l'integratità e la disponibiltà. 0=nessun impatto 1=basso 2=medio 3=alto	3	2	1	(esempio)
Risorse e asset correlati				
Processo				
Prodotto/Servizio				
Hardware/Rete				
Software				
Osservazioni				
Modivare i valori attribuiti alle dimensioni dell' asset in modo che l'analisi sia riproducibile				

figura 6

Il range dei valori spazia da 3 (= massimo impatto) a 1 (= minimo) valutato rispettivamente su un'eventuale perdita di riservatezza (a_ris), dell'integrità (a_int) e della disponibilità (a_disp).
La valutazione di eventuali risorse correlate servirà al consulente per considerazioni aggiuntive riguardo alla natura strategica delle interdipendenze ravvisate.

Nonostante l'importanza attribuita dal Regolamento Europeo alla sicurezza informatica (ai sensi dell' art. 32), non è raro incontrare consulenti che ritengano sufficiente l'ispezione documentale per formulare un giudizio di conformità.
Un approccio del genere, tra l'altro, dimostra di non tenere in debito conto neanche i concetti di *privacy by design* e *privacy by default* che insistono nel considerare la dimensione della security come una variabile strategica, da integrare profondamente all'interno dell'organizzazione anche a costo di profondi cambiamenti nella struttura.

Tutto il quadro normativo infatti, va letto nella duplice ottica da un lato della protezione del dato come estrinsecazione di un diritto fondamentale, dall'altro della protezione del dato in quanto avente *un valore economico*, il dato come *informazione* che transita in un sistema intrinsecamente fallibile che va hardenizzato e messo in sicurezza per mantenere alta la fiducia degli attori coinvolti e mantenere una posizione privilegiata nei mercati internazionali.
Il security audit viene così a configurarsi come l'altra faccia della medaglia, dimensione imprescindibile per una lettura corretta delle modalità operative di un trattamento di dati personali.
Il check sulla sicurezza si articola su domande, molte delle quali autoesplicative, relative a 5 macroaree:

1. La **sicurezza fisica dei locali**

•

Security Audit - Sicurezza fisica dei locali				
La scheda ha l'obiettivo di tenere sotto controllo gli archivi fisici e digitali				
Gli archivi fisici dove i dati in formato cartaceo di questo trattamento vengono custoditi sono organizzati in moduli ordinati e facilmente	si	no		
I dati cartacei e digitali sono custoditi in armadio chiuso a chiave (rack) ?	si	no		
I locali dove vengono consultati o manipolati i dati in questione è a libero accesso?	si	no		
I soggetti che hanno accesso ai documenti sono identificati	si	no		
Esiste personale di sorveglianza ?	si	no		
Esistono videocamere di sorveglianza ?	si	no		
I locali dove risiedono gli apparati di rete e i server sono adeguatamente condizionati e manutenuti?	si	no		
I cablaggi sono etichettati e dotati di UPS?	si	no		
Osservazioni				
valutazione sulle misure antincendio e di sic con riferimento alla normativa vigente				

FIGURA 7

2. La **sicurezza dei sistemi informatici**

Security Audit - Sicurezza dei sistemi informatici				
La scheda ha l'obiettivo di tenere sotto controllo l'accesso alle informazioni dei sistemi informatici				
I sistemi informatici coinvolti nella gestione dei dati del trattamento sono dotati di controllo degli accessi centralizzato?	si	no		
Il personale autorizzato all'accesso dispone di credenziali personali con privilegi profilati, non condivise con altri e aggiornate nelle	si	no		
I sistemi sono configurati per generare password di sufficiente complessità, richiedendone la variazione ad intervalli periodici (almeno ogni	si	no		
Ogni utente accede solo alle informazioni di sua competenza	si	no		
Quanto tempo vengono conservati i log?	si	no		
Sulle postazioni informatiche vengono create	si	no		
Vengono periodicamente effettuati backup che consentano il ripristino immediato delle funzionalità a seguito di un incidente	si	no		
Il SO, il suo firewall e l'antivirus sono periodicamente aggiornati e configurati con le opportune estensioni che consentano la rilevazione di	si	no		
Amministratore di sistema *(facoltativo)*				
Osservazioni *(valutazione sul grado reale di consapevole personale addetto)*				

FIGURA 8

3. La **sicurezza della rete**

Security Audit - Sicurezza della rete				
La scheda ha l'obiettivo di tenere sotto controllo le connessioni di rete				
Il flusso di elaborazione del dato oggetto del trattamento risiede solo sulla rete interna o esistono punti di contatto con l'esterno?				
E' presente una connessione WIFI separata per uso interno e per ospiti?	si	no		
Esistono firewall o altri sistemi per filtrare/monitorare accessi non autorizzati				
Esistono strumenti specifici anti-intrusione?	si	no		
La policy aziendale vieta hotspot con smartphone	si	no		
Altro				
Amministratore di rete				
Osservazioni				

FIGURA 9

4. Scheda di **controllo del sito web**

Sito Web - Scheda di conformità					
La scheda ha l'obiettivo di tenere sotto controllo la conformità del sito web da cui entrano i dati del trattamento					
Il sito web acquisisce i dati attraverso un form di registrazione ?	si	no			
Esistono nel form campi non necessari o text area che potrebbero iniettare dati sensibili?	si	no			
L'invio della registrazione è subordinato alla presa visione dell'informativa sul trattamento e al consenso della cookie policy?	si	no			
I dati richiesti dal form e registrati sono solo quelli necessari alle finalità	si	no			
Il sito incorpora procedure per la cancellazione/modifica /esportazione dati	si	no			
La società esterna che ha realizzato/può accedere il/al sito è stata tracciata con contratto di responsabilizzazione	si	no			
Esiste una procedura per aggiornare periodicamente il software applicativo	si	no			
Esiste un monitoraggio periodico delle vulnerabilità	si	no			
Il database del sito è crittografato ed è sottoposto a periodici backup	si	no			
	si	no			
Osservazioni					

FIGURA 10

5. **Formazione sulle best practices di sicurezza delle risorse umane**

Chi scrive sa bene che la formazione del personale non può ridursi ad un semplice questionario da far sottoscrivere ma è un'attività cruciale, complessa, multisfaccettata, afferente a tutti i livelli della catena logistica e organizzativa.
Spesso sono proprio gli impiegati distratti o delusi che inconsapevolmente o consapevolmente mettono in atto comportamenti che spalancano le porte dei nostri sistemi alle pratiche illecite dei criminali informatici.

Security Audit - Scheda formazione del personale			
La scheda ha l'obiettivo di dimostrare di aver formato gli incaricati del trattamento sulle best practices di sicurezza delle informazioni.			
Data			
Nome Cognome Incaricato			
Come soggetto operativo su una base informativa contenente dati personali ritengo di essere investito di una grande responsabilità	si	no	non so
Considero le minacce all'integrità del dato una realtà di fronte alla quale presto continuamente la massima attenzione	si	no	non so
Per accedere al terminale utilizzo un meccanismo di autenticazione	si	no	non so
La password con cui accedo al terminale è a mio uso esclusivo e conservata in luogo sicuro	si	no	non so
Utilizzo un'autenticazione a due fattori	si	no	non so
Non utilizzo la stessa password per più di un account	si	no	non so
Cambio la password di accesso alla mia postazione con periodicità costante	si	no	non so
Non utilizzo account personali sui terminali aziendali	si	no	non so
Non mi connetto alla rete aziendale con devices personali (smartphone, tablet)	si	no	non so
Presto attenzione allo stato di sicurezza del mio terminale: se vedo avvisi o messaggi di aggiornamento contatto	si	no	non so
Sui terminali aziendali eseguo solo attività legate al mio ruolo, su applicazioni e indirizzi web consentiti	si	no	non so
Sui terminali aziendali eseguo solo attività legate al mio ruolo, su applicazioni e indirizzi web consentiti	si	no	non so
Presto la massima attenzione alle mail che ricevo: se contengono link valuto accuratamente la provenienza; se ci sono allegati, prima li salvo su disco, poi li controllo con l'antivirus e solo alla fine li apro.	si	no	non so
Aggiungi piè di pagina			
Aggiungi intestazione			
Sono a conoscenza che, se mi connetto con il cellulare alla rete aziendale e clicco con il mio account personale su un allegato infetto il malware può diffondersi all'interno della rete	si	no	non so
Se noto anomalie nei files o lentezze particolari mi rivolgo subito all'AdS.	si	no	non so
Non utilizzo supporti esterni personali o comunque non inventariati dal AdS	si	no	non so
Chiedo regolarmente all'AdS di verificare l'aggiornamento del mio terminale e il controllo/verifica del backup	si	no	non so
Diffido delle mail che mi richiedono di fornire dati personali o di aggiornare presunti account bancari o postali e di chiamare call center per risolvere problemi amministrativi. Prima di agire verifico con gli interlocutori coinvolti.	si	no	non so
Non condivido alcuna informazione personale sui social che possa essere semanticamente sfruttata da un attaccante per violare il mio account.			
Svincolo la mia password dai miei interessi, hobbies, legami familiari,anche	si	no	non so
Non mi connetto alla rete aziendale con devices personali (smartphone, tablet)	si	no	non so
Presto attenzione allo stato di sicurezza del mio terminale: se vedo avvisi o messaggi di aggiornamento contatto	si	no	non so
Sui terminali aziendali eseguo solo attività legate al mio ruolo, su applicazioni e indirizzi web consentiti	si	no	non so
Presto la massima attenzione alle mail che ricevo: se contengono link valuto accuratamente la provenienza; se ci sono allegati, prima li salvo su disco, poi li controllo con l'antivirus e solo alla fine li apro.	si	no	non so
Firma Incaricato			

Tuttavia il questionario proposto nel presente lavoro costituisce un ottimo strumento, già am-

piamente testato, per iniziare ad introdurre i concetti di sicurezza informatica sopratutto nelle piccole realtà, di solito inconsapevoli, traendo un utile spunto per incontri più approfonditi e verticalizzati.

Come anticipato in precedenza, la valutazione congiunta delle schede di audit porta l'analista ad attribuire un punteggio ai controlli:

- **3** = controllo sotto la media - alta vulnerabilità
- **2** = controllo nella media
- **1** = controllo sopra la media - bassa vulnerabilità

IL PROCESSO DI RISK ASSESSMENT

Il Regolamento Europeo sulla protezione dei dati introduce nel mondo legislativo della privacy un approccio *risk based*.
Come già ampiamente discusso, non esistono più misure *minime,* attraverso le quali sia possibile far passare "per buoni" trattamenti solo formalmente conformi alla legge. Oggi un titolare ha l'onere di prendere in considerazione il rischio generato da un trattamento sui diritti e le libertà degli interessati e di mettere in atto tutte le misure ritenute *adeguate* a contenerne l'impatto stimato.
Non è un cambiamento da poco. A molti "burocrati" della privacy non piace.
L'audit ai sensi del GDPR non può più essere un semplice e statico confronto con l'allegato B del Codice ma deve prevedere un *atto* di presa di coscienza del titolare, il quale, nel nome del principio di accountability, assume su di sè i rischi del trattamento, li valuta, li pondera e li *monitora* , in un continuo processo dinamico che lo vede protagonista attivo e parte integrante della tutela degli interessati a cui si rivolge.

La metodologia presentata in questo lavoro propone un approccio all'analisi del rischio di tipo qualitativo (non esistendo tabelle attuariali sulle cyber minacce) arricchito da note e richiami dell'analista alle statistiche ufficiali (ad esempio il Rapporto Clusit) e alle riviste del settore, al fine di garantire il più possibile un margine di ripetibilità e intersoggettività.

La metrica suggerita è articolata in 3 classi:
- 1= basso rischio intrinseco
- 2= medio rischio insinseco
- 3= alto rischio intrinseco

che il trattamento possa ledere il diritto fondamentale degli interessati.

Una volta effettuato il *prodotto logico* del livello individuato di rischio intrinseco del trattamento per gli adempimenti normativi e le misure di sicurezza implementate durante il ciclo di vita dell'asset, la fase di ponderazione stabilirà se il livello di rischio *totale* sia o meno accettabile per il Titolare del trattamento, producendo come conseguenza eventuali misure di trattamento del rischio e relativo monitoraggio. I criteri di accettabilità sono quelli che bilanciano il rischio di

impresa e la sua sostenibilità in termini economici.

IDENTIFICAZIONE, ANALISI E PONDERAZIONE DEL RISCHIO

Obiettivo di questa fase è di popolare la matrice del rischio per il calcolo dell'equazione.
I dati di input necessari all'analista sono:

- l'impatto dell'asset (determinato nella fase iniziale del security audit) che chiameremo z(a) con z(a)= (z_a_ris, z_a_disp, z_a_int) nelle tre dimensioni CIA.
- l'impatto della minaccia iesima z_i(m), con z(m)=(z_m_ris, z_m_disp, z_m_int)
- la probabilità di occorrenza della minaccia p(m_i)

La matrice del rischio intrinseco si ottiene con la formula

R(m,a) = max { p(m) * z(m) * z(a) } con z= (z_ris, z_disp, z_int).

Ad esempio, se p(m)=2, z(m) =(0,1,1), z(a) = (2,2,3)
Ri(a)= max {(2*0*2),(2*1*2), (2*1*3) } = max (0,4,6) = 6 .

Calcolo del rischio intrinseco

Formula R(m,a) = max { p(m) * z(m) * z(a) } con z= (z_ris, z_disp, z_int). Ad esempio, se p(m)=2, z(m) =(0,1,1), z(a) = (2,2,3) Ri(a)= max {(2*0*2),(2*1*2), (2*1*3) } = max (0,4,6) = 6 . Tale calcolo verrà ripetuto per ogni risorsa correlata al trattamento e come rischio intrinseco del trattamento verrà considerato il valore massimo. **Basso rischio intrinseco = 0-6 Medio rischio intrinseco 7-12 Alto rischio intrinseco = 13-27 (tenere traccia della risorsa con il livello di rischio più alto).**

Punteggio di vulnerabilità *(assegnato in seguito a valutazione globale dei due audit)* ***3=controllo sotto alla media 2= controllo nella media 1= controllo oltre la media.***

necessario un trattamento se > 36

Asset	Rischio intrinseco	Vulnerabilità	Rischio totale (R*V)

FIGURA 11

Tale calcolo verrà ripetuto (FIGURA 11) per ogni risorsa correlata al trattamento e per ogni minaccia e come rischio intrinseco del trattamento verrà considerato il *valore massimo*.

La mappatura tra il valore così ottenuto e la metrica di analisi può essere considerata la seguente:

1. Basso rischio intrinseco = 0-6
2. Medio rischio intrinseco 7-12
3. Alto rischio intrinseco = 13-27

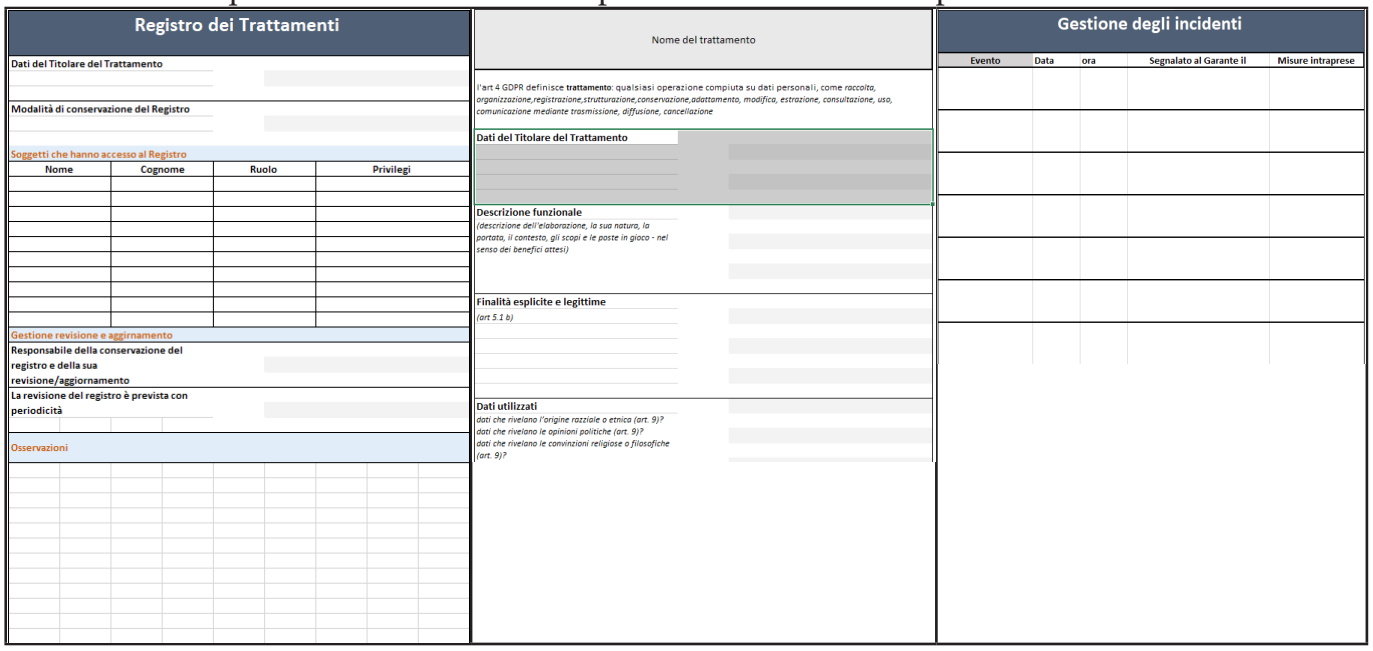
Per determinare il livello di rischio *totale*, il valore di rischio intrinseco viene moltiplicato per il livello di controllo emerso dalla valutazione congiunta degli audit.

Se il punteggio che si ottiene supera una certa soglia di accettabilità (nella metrica qui esposta ad esempio, il valore 36), l'impatto del trattamento è considerato alto, l'analista suggerisce al titolare di redarre un piano di trattamento del rischio e di procedere con la valutazione di impatto (dpia) prevista dall'articolo 35 del Regolamento.

In ogni caso, la fase di ponderazione rappresenta strettamente una decisione del titolare, il quale può discostarsi dai suggerimenti dell'analista, purchè tale scelta sia opportunamente motivata. Il criterio di accettabilità del rischio infatti è quello che bilancia il rischio di impresa e la sua sostenibilità in termini economici.
L'importante, ai fini della conformità sostanziale al Regolamento, è che il titolare prenda in considerazione i rischi e che la sua decisione sia consapevole e ragionata.

IL REGISTRO DEI TRATTAMENTI

Una volta determinato il rischio del trattamento il Titolare può, con l'aiuto del consulente, procedere a redarre il Registro ai sensi dell'art. 30.
In questa sede proponiamo un modello di Registro non minimale, in cui l'analisi dei trattamenti, unitamente alla documentazione che si arriva a gestire grazie alla metodologia illustrata, è molto vicina a quella richiesta dal WP29 per la valutazione di impatto.



Registro dei Trattamenti

Dati del Titolare del Trattamento

Modalità di conservazione del Registro

Soggetti che hanno accesso al Registro

Nome	Cognome	Ruolo	Privilegi

Gestione revisione e aggiornamento

Responsabile della conservazione del registro e della sua revisione/aggiornamento

La revisione del registro è prevista con periodicità

Osservazioni

Nome del trattamento

l'art 4 GDPR definisce **trattamento**: qualsiasi operazione compiuta su dati personali, come *raccolta, organizzazione,registrazione,strutturazione,conservazione,adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, cancellazione*

Dati del Titolare del Trattamento

Descrizione funzionale
(descrizione dell'elaborazione, la sua natura, la portata, il contesto, gli scopi e le poste in gioco - nel senso dei benefici attesi)

Finalità esplicite e legittime
(art 5.1 b)

Dati utilizzati
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)?

Gestione degli incidenti

Evento	Data	ora	Segnalato al Garante il	Misure intraprese

Troviamo infatti:

- la descrizione sistematica del trattamento con riguardo ai principi di liceità, correttezza, trasparenza, minimizzazione;
- la descrizione del flusso e la mappatura delle risorse sull'infrastruttura operativa;
- l'analisi del rischio, descritta in dettaglio nel paragrafo precedente;
- un prospetto per gestire gli incidenti e tracciare le misure implementate per minimizzare l'impatto e l'eventuale comunicazione al Garante.

OSSERVAZIONI CONCLUSIVE E PROSPETTIVE DI MIGLIORAMENTO

Il presente lavoro nasce "dal campo" e cerca di rispondere all'esigenza degli operatori del settore di dotarsi di linee guida metodologiche per affrontare l'audit ai sensi del Gdpr in tutta la sua complessità, come riteniamo emerga chiaramente dalla discussione affrontata.

Una prospettiva di miglioramento della metodologia proposta è di inserire nel piano di trattamento i *test di vulnerabilità* e *metriche* per facilitarne il monitoraggio dello stato dell'arte.

Chi scrive è un analista informatico che conosce bene la complessità del vulnerability assessment e la conseguente difficoltà ad introdurre questi concetti in realtà come le PMI, strette nella morsa del cibercrime ma non aventi il budget per dotarsi di un adeguata sovrastruttura protettiva.

La sfida è proprio quella di realizzare un format applicabile anche alle realtà meno consapevoli avvicinandole a concetti cruciali per mantenersi competitive nella nostra società infocentrica e interagire con tranquillità nello spazio cyber delle transazioni.

Istruzioni su come usare il Modello

Identificare i trattamenti con l'aiuto della scheda

Identificazione dei trattamenti

Per ogni trattamento identificato, compilare le seguenti schede:

Privacy Audit

1 Descrizione Sistematica del Trattamento

Security Audit

2 Scheda sul Security Audit

2.a	Scheda Asset Management
2.b	Scheda Sicurezza fisica dei locali
2.c	Scheda sulla gestione sistemi informativi
2.d	Scheda sicurezza della rete
2.e	Scheda sulla formazione del personale

3 Controllo sulla conformità dell'informativa

4 Scheda controllo sito web come entry point

Assegnazione punteggio all'audit: 3= controllo sotto la media, 2 = nella media 1= sopra la media

Valutazione dei rischi

5 Scheda Identificazione del rischio

6 Scheda Analisi e Impatto Rischio

7 Scheda Ponderazione / trattamento del Risch

Una volta ottenute le informazioni, si procede alla compilazione della scheda finale

Scheda finale del trattamento (da inserire nel Registro)

Identificare i possibili trattamenti (elenco non esaustivo)

l'art 4 GDPR definisce **trattamento**: qualsiasi operazione compiuta su dati personali, come *raccolta, organizzazione,registrazione,strutturazione,conservazione,adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, cancellazione*

Dati di dipendenti	
(attuali o potenziali)	trattamento a scopo di assunzione
	tratt.amministrativo relativo al rapporto di lavoro
	tratt. A scopo di monitoraggio curricolare
	tratt. Ai fini di controllo prestazione lavorativa -videosorveglianza
	tratt. Con finalità extralavorativa (ricreativa)
	tratt. Con finalità di formazione
	trattamento a scopo di donazione verso terzi
	trattamento a scopo di protezione attraverso monitoraggio rete
Dati di fornitori	
	trattamento a scopo amministrativo (gestione ordine/fatture)
	tratt invio contenuti tramite newsletter
	tratt. A scopo di invio materiale pubblicitario
	tratt. A scopo di soluzione di una controversia
	tratt. Con finalità richiesta audit di sicurezza
	trattamento a scopo di donazione verso terzi
Dati di clienti	trattamento per adempimento contratto
(anche interessati per conto di altri)	trattamento a scopo amministrativo (gestione ordini/fatture)
	tratt invio contenuti tramite newsletter
	tratt. A scopo di invio materiale pubblicitario
	tratt. A scopo di soluzione di una controversia
	tratt. Con finalità richiesta audit di sicurezza
	trattamento a scopo di donazione verso terzi

Nome del trattamento

l'art 4 GDPR definisce **trattamento**: qualsiasi operazione compiuta su dati personali, come *raccolta, organizzazione,registrazione,strutturazione,conservazione,adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, cancellazione*

Dati del Responsabile

(opzionale)

Descrizione funzionale

(descrivere il flusso del trattamento)

Finalità esplicite e legittime

(ex per finalità amministrative o di marketing)

Dati utilizzati

1) Esaminare se il trattamento riguarda dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche o religiose, l'appartenenza sindacale, dati genetici o biometrici, relativi alla salute o alla vita sessuale. In tale caso sarà necessario il consenso **esplicito** *ex art. 9 del GPDR*

2) Esaminare se vengono trattati dati giuridici relativi a condanne penali. In genere il trattamento non è consentito salvo art 21 e 27 cod. Privacy e doc web Garante 3632788

3) se dati sanitari del lavoratore, conservare in fascicoli separati ed è vietata la diffusione

Casi di esonero verifica preliminare

4) se dati biometrici doc web 3556992-3563006

presidio accesso utilizzo sistemi critici

Categoria di interessato

1) Se siamo di fronte ad un trattamento di dati di dipendenti valutare la conformità al D. Legisl. 2015 n 151 rispondendo alle domande in blu

Durata

Viene fatto ricorso a risorse esterne a cui affidare i dati ? Sono stati nominati responsabili esterni del trattamento ?
(allegare contratto di nomina)

si no

si no

Individuazione delle risorse coinvolte
(indicare il computer dove risiede il database e i computer ad esso collegati)

Hardware

(indicare i programmi che si utilizzano per operare e accedere ai dati - ad esempio google drive, dropbox ecc)

Software

Incaricati /segmento di rete

Nome	Cognome

Valutazione sulla liceità *(art 6 GDPR 1)consenso 2)esecuzione di un contratto 3)obbligo legale 4) interessi vitali dell'interessato o altra persona 5) interesse pubblico o pubblici poteri 6) legittimo interesse)*		
E' stata data adeguata informativa ? *(art 13 - 14 GDPR fornisce i contenuti obbligatori)*	si	no
Il consenso è stato richiesto in forma comprensibile e separata dal contesto?*(art*	si	no
Comunicazione dei dati a terzi *(necessità di informativa art 13 sui destinatari e consenso se fondamento di liceità)*	si	no
Trasferimento dati a paesi extra UE *(ex art 44 GDPR ammesso solo se garantito adeguato livello di protezione o in base ad una decisione di adeguatezza (art 45)*	si	no
I dati raccolti sono adeguati, limitati e pertinenti rispetto a quanto necessario in base alle finalità, esatti e aggiornati? *(art 5 sui principi-liceità, correttezza, trasparenza)*		
La conservazione dei dati sarà limitata alla durata del trattamento rispettando il principio di minimizzazione e grazie a procedure codificate ? *(Art 5 sul principio di minimizzazione della conservazione)*	si	no
Il trattamento prevede procedure che garantiscono diritto di accesso/modifica *(art 15 - 16)*	si	no
Il trattamento prevede procedure che garantiscono diritto di portabilità *(art 20)*	si	no
Il trattamento prevede procedure che garantiscono diritto di oblio /opposizione *(art 17-21)*	si	no

I contratti degli incaricati del trattamento prevedono apposite clausole di riservatezza *(allegare dei campioni)*	si	no

Eventuali fornitori a cui i dati vengono trasmessi hanno firmato specifico contratto di responsabilizzazione *(in allegato)*	si	no
Il Titolare utilizza i dati acquisiti per la finalità di questo trattamento in mailing list avente altra finalità? *Verificare che la presenza della richiesta di consenso e la possibilità di opporsi alla mailing list sia ben evidente nell'informativa, separatamente da ogni altra informazione (art 21, comma 4 -diritto di opposizione)*	si	no
Trattamento di dati personali dei lavoratori		
Il trattamento prevede l'adozione di un disciplinare interno ***(linee Guida Garante sull'utilizzo di intenet e della posta elettronica)***	si	no
Il Titolare ha prodotto specifica informativa sulla politica di utilizzo di internet ***(linee Guida Garante sull'utilizzo di intenet e della posta elettronica)***	si	no
Il Trattamento non usa strumenti che consentano un controllo intenzionale a distanza dell'attività del lavoratore. *Es lettura e registrazione automatica dei messaggi di posta elettronica o della cronologia internet*	si	no
Il Trattamento non usa strumenti che consentano un controllo intenzionale a distanza dell'attività del lavoratore. *Es videosorveglianza o dispositivi di geolocalizzazione* *Se c'è videosorveglianza per scopi di sicurezza allegare accordo sindacale o autorizzazione Ispettorato ex D. Leg 151/2015* *se la geolocalizzazione è richiesta per motivi di sicurezza i dati a cui il titolare ha accesso sono quelli ispirati al principio di minimizzazione e ben visibili al lavoratore*	si si	no no

Informativa - Scheda di controllo sulla conformità

La scheda ha l'obiettivo di prendere in considerazione la finalità del trattamento, le categorie di dati trattati e altre informazioni utili per valutare la conformità dell'informativa fornita ed eventualmente la necessità di consenso esplicito.

Linee guida per la compilazione dell'informativa

Contenuto minimo

Finalità e modalità del trattamento

quali categorie di dati vengono trattate, per quali fini, per quanto tempo, se vengono trasmessi all'estero o a terzi e attraverso quali strumenti.

Natura obbligatoria o facoltativa del conferimento dati

specificare se il soggetto possa o meno rifiutare il consenso e, in caso affermativo, quali siano le conseguenze del rifiuto.

Informazione all'interessato circa i suoi diritti

in particolare sulla possibilità di aver accesso ai suoi dati, modificarli, richiederne la cancellazione, la consegna in formato strutturato, e di presentare richiamo all'Autorità di Controllo

Dati identificativi del Titolare del trattamento

nome, ragione sociale, sede legale, indirizzo di contatto

Dati identificativi del Responsabile del trattamento

nome, ragione sociale, sede legale, indirizzo di contatto

Dati identificativi delResponsabile della Protezione dei Dati

nome, ragione sociale, sede legale, indirizzo di contatto

La base giuridica del trattamento

Specificare se basato sul consenso oppure giustificato dalla legge o altro fondamento di liceità .

Informazione circa eventuale profilazione

Se l'utilizzo comporta profilazione, nel senso di trattamenti decisionali automatizzati (cioè senza l'intervento umano) che causino conseguenze giuridiche rilevanti, specificarne gli algoritmi e la logica.

Informazione sugli eventuali destinatari categorie di destinatari dei dati personali

Intenzione del titolare di trasferire dati personali ad un paese terzo

Ciò è possibile in presenza di una decisione di adeguatezza della Commissione circa le garanzie attuate dal paese in questione

Informazione sul diritto di revocare il consenso al trattamento in qualsiasi momento

Cookies

Se i dati trattati entrano via web specificare il tipo di cookies che veicola il sito, la possibilità di disabilitarli tramite browser e, nel caso di cookies di terzi, il link al sito con la privacy policy relativa

Nel caso di dati sensibili è necessario il consenso esplicito e, se l'interessato ha meno di 16 anni quello dei genitori (eventualmente richiedere una autodichiarazione sull'età). Il consenso deve essere libero, verificabile e derogabile, attraverso opportune procedure

Security Audit - scheda introduttiva

Il check preliminare ha l'obiettivo di fotografare lo stato attuale della struttura sotto il profilo della sicurezza dei dati trattati. I controlli di sicurezza si ispirano a quelli consigliati dal framework nazionale NIST. Compilare tante schede quanti sono gli asset informativi da valutare

Dati dell'Auditor

Asset da proteggere
(Informazione-processo-prodotto)

Valore attribuito
parametri: assegnare un valore da 0 a 3 all'asset, a secondo dell'impatto che si avrebbe sui diritti dell'interessato se venisse meno la riservatezza, l'integratità e la disponibiltà.
0=nessun impatto 1=basso 2=medio 3=alto

a_ris	a_int	a_disp	
3	2	1	(esempio)

Risorse e asset correlati

Processo

Prodotto/Servizio

Hardware/Rete

Software

Osservazioni
Modivare i valori attribuiti alle dimensioni dell' asset in modo che l'analisi sia riproducibile

Compilare per ciascun asset le schede relative a Asset Management, Sicurezza dei locali fisici, Sicurezza dei sistemi informativi e sicurezza della rete.

Security Audit - Asset Management

La scheda ha l'obiettivo di tenere sotto controllo i dati oggetto di trattamento durante l'intero ciclo di vita

Esiste ed è mantenuto aggiornato un inventario di dispositivi, software, servizi e applicazioni informatiche che utilizzano l'asset?	si	no
Il dato è trasmesso a servizi web di terze parti ?	si	no
Dati dell'Azienda esterna/Responsabile		
Esiste un contratto di nomina esplicito?	si	no
Si dispone di report/certificazioni sulla sicurezza del fornitore?	si	no
Esiste un referente / responsabile dell'aggiornamento dell'inventario	si	no
Il personale coinvolto nella gestione dei dati è stato informato sulle best practices di sicurezza *(scheda formazione del personale + meetings di formazione verbalizzati)*	si	no
Osservazioni		

Security Audit - Sicurezza fisica dei locali

La scheda ha l'obiettivo di tenere sotto controllo gli archivi fisici e digitali

Gli archivi fisici dove i dati in formato cartaceo di questo trattamento vengono custoditi sono organizzati in moduli ordinati e facilmente consultabili ?	si	no
I dati cartacei e digitali sono custoditi in armadio chiuso a chiave (rack) ?	si	no
I locali dove vengono consultati o manipolati i dati in questione è a libero accesso?	si	no
I soggetti che hanno accesso ai documenti sono identificati ed identificabili ?	si	no
Esiste personale di sorveglianza ?	si	no
Esistono videocamere di sorveglianza ?	si	no
I locali dove risiedono gli apparati di rete e i server sono adeguatamente condizionati e manutenuti?	si	no
I cablaggi sono etichettati e dotati di UPS?	si	no
Osservazioni *valutazione sulle misure antincendio e di sicurezza con riferimento alla normativa vigente*		

Security Audit - Sicurezza dei sistemi informatici

La scheda ha l'obiettivo di tenere sotto controllo l'accesso alle informazioni dei sistemi informatici

I sistemi informatici coinvolti nella gestione dei dati del trattamento sono dotati di controllo degli accessi centralizzato?	si	no
Il personale autorizzato all'accesso dispone di credenziali personali con privilegi profilati, non condivise con altri e aggiornate nelle corrette attribuzioni	si	no
I sistemi sono configurati per generare password di sufficiente complessità, richiedendone la variazione ad intervalli periodici (almeno ogni 6 mesi) ?	si	no
Ogni utente accede solo alle informazioni di sua competenza	si	no
Quanto tempo vengono conservati i log?	si	no
Sulle postazioni informatiche vengono create periodicamente immagini di	si	no
Vengono periodicamente effettuati backup che consentano il ripristino immediato delle funzionalità a seguito di un incidente informatico?	si	no
Il SO, il suo firewall e l'antivirus sono periodicamente aggiornati e configurati con le opportune estensioni che consentano la rilevazione di malware e la navigazione sicura?	si	no
Amministratore di sistema *(facoltativo)*		
Osservazioni *(valutazione sul grado reale di consapevolezza del personale addetto)*		

Security Audit - Sicurezza della rete

La scheda ha l'obiettivo di tenere sotto controllo le connessioni di rete

Il flusso di elaborazione del dato oggetto del trattamento risiede solo sulla rete interna o esistono punti di contatto con l'esterno?

E' presente una connessione WIFI separata per uso interno e per ospiti? si no

Esistono firewall o altri sistemi per filtrare/monitorare accessi non autorizzati

Esistono strumenti specifici anti-intrusione?

si no

La policy aziendale vieta hotspot con smartphone personali si no

Altro

Amministratore di rete

Osservazioni

Security Audit - Scheda formazione del personale

La scheda ha l'obiettivo di dimostrare di aver formato gli incaricati del trattamento sulle best practices di sicurezza delle informazioni.

Data			
Nome Cognome Incaricato			
Come soggetto operativo su una base informativa contenente dati personali ritengo di essere investito di una grande responsabilità	si	no	non so
Considero le minacce all'integrità del dato una realtà di fronte alla quale presto continuamente la massima attenzione	si	no	non so
Per accedere al terminale utilizzo un meccanismo di autenticazione	si	no	non so
La password con cui accedo al terminale è a mio uso esclusivo e conservata in luogo sicuro	si	no	non so
Utilizzo un'autenticazione a due fattori	si	no	non so
Non utilizzo la stessa password per più di un account	si	no	non so
Cambio la password di accesso alla mia postazione con periodicità costante	si	no	non so
Non utilizzo account personali sui terminali aziendali	si	no	non so
Non mi connetto alla rete aziendale con devices personali (smartphone, tablet)	si	no	non so
Presto attenzione allo stato di sicurezza del mio terminale: se vedo avvisi o messaggi di aggiornamento contatto l'AdS	si	no	non so
Sui terminali aziendali eseguo solo attività legate al mio ruolo, su applicazioni e indirizzi web consentiti	si	no	non so
Presto la massima attenzione alle mail che ricevo: se contengono link valuto accuratamente la provenienza; se ci sono allegati, prima li salvo su disco, poi li controllo con l'antivirus e solo alla fine li apro.	si	no	non so

Sono a conoscenza che, se mi connetto con il cellulare alla rete aziendale e clicco con il mio account personale su un allegato infetto il malware può diffondersi all'interno della rete aziendale	si	no	non so
Se noto anomalie nei files o lentezze particolari mi rivolgo subito all'AdS.	si	no	non so
Non utilizzo supporti esterni personali o comunque non inventariati dal AdS	si	no	non so
Chiedo regolarmente all'AdS di verificare l'aggiornamento del mio terminale e il controllo/verifica del backup	si	no	non so
Diffido delle mail che mi richiedono di fornire dati personali o di aggiornare presunti account bancari o postali e di chiamare call center per risolvere problemi amministrativi. Prima di agire verifico con gli interlocutori coinvolti.	si	no	non so
Non condivido alcuna informazione personale sui social che possa essere semanticamente sfruttata da un attaccante per violare il mio account. Svincolo la mia password dai miei interessi, hobbies, legami familiari,anche con tool automatici	si	no	non so
Non mi connetto alla rete aziendale con devices personali (smartphone, tablet)	si	no	non so
Presto attenzione allo stato di sicurezza del mio terminale: se vedo avvisi o messaggi di aggiornamento contatto l'AdS	si	no	non so
Sui terminali aziendali eseguo solo attività legate al mio ruolo, su applicazioni e indirizzi web consentiti	si	no	non so
Presto la massima attenzione alle mail che ricevo: se contengono link valuto accuratamente la provenienza; se ci sono allegati, prima li salvo su disco, poi li controllo con l'antivirus e solo alla fine li apro.	si	no	non so
Firma Incaricato			

Sito Web - Scheda di conformità

La scheda ha l'obiettivo di tenere sotto controllo la conformità del sito web da cui entrano i dati del trattamento

Il sito web acquisisce i dati attraverso un form di registrazione ?	si	no
Esistono nel form campi non necessari o text area che potrebbero iniettare dati sensibili?	si	no
L'invio della registrazione è subordinato alla presa visione dell'informativa sul trattamento e al consenso della cookie policy?	si	no
I dati richiesti dal form e registrati sono solo quelli necessari alle finalità	si	no
Il sito incorpora procedure per la cancellazione/modifica /esportazione dati	si	no
La società esterna che ha realizzato/può accedere il/al sito è stata tracciata con contratto di responsabilizzazione	si	no
Esiste una procedura per aggiornare periodicamente il software applicativo	si	no
Esiste un monitoraggio periodico delle vulnerabilità	si	no
Il database del sito è crittografato ed è sottoposto a periodici backup	si	no
	si	no
Osservazioni		

Risk Assessment - Identificazione del rischio

Partendo dal valore attribuito all'asset informativo investito dal trattamento sulla scheda introduttiva e prendendo in input il security audit, questo modulo mira ad identificare le minacce e le vulnerabilità

Criteri di rischio

La valutazione del rischio segue una metodologia di tipo qualitativo. La metrica sarà articolata in 3 classi: **1= basso rischio 2= medio rischio 3= alto rischio che il trattamento possa ledere il diritto fondamentale alla riservatezza degli interressati**. Una volta determinato il livello di rischio del trattamento, dati gli adempimenti normativi e le misure di sicurezza implementati durante il ciclo di vita dell'asset, la fase di ponderazione stabilirà se il livello di rischio è accettabile per il Titolare del trattamento, producendo come conseguenza eventuali misure di trattamento del rischio e relativo monitoraggio. **I criteri di accettabilità sono quelli che bilanciano il rischio di impresa e la sua sostenibilità in termini economici.**

Applicabilità al contesto del trattamento delle seguenti minacce		
Intrusione non autorizzata nella sede del trattamento	si	no
Intrusione non autorizzata nei sistemi informatici	si	no
Furto di credenziali e di informazioni attraverso social engineering	si	no
Danneggiamento di apparecchiature per cause naturali, tecniche, errori umani	si	no
Danneggiamento dei sistemi informatici per attacchi , ragioni tecniche o cause nat.	si	no
Furto di dispositivi	si	no
furto, lettura, copia non autorizzata di documenti fisici	si	no
Lettura, furto o modifica non autorizzata di documenti digitali	si	no
Malware	si	no
Copia e uso illegale di software	si	no
Uso non autorizzato di servizi internet esterni	si	no
Trattamento dei dati non conforme da parte dei fornitori di servizi	si	no
Recupero di dati da supporti dismessi	si	no
Esaurimento o riduzione delle risorse informatiche (Ddos, web defacement)	si	no
Intercettazione delle comunicazioni, sabotaggio e furto di proprietà intellett.	si	no

Invio non autorizzato di dati a terzi	si	no
Invio e ricezione di dati non sottocontrollo (sql injection)	si	no

Motivazioni: (con aiuto di interviste al Responsabile del Trattamento su quanto già verificatosi)

Risk Assessment - Analisi del rischio

Questa scheda prende in input 1) le minacce considerate applicabili al contesto del trattamento, definite nella scheda di identificazione, 2) i risultati del security audit e 3) i valori assegnati ai parametri dell'asset oggetto del trattamento e ottiene in output il livello di rischio attuale del trattamento

Recupero parametri degli asset *(definiti sulla scheda security audit introduttiva)*

	a_ris	a_int	a_disp
Flusso dati principale (asset informativo)			
(base informativa oggetto del trattamento)			
Risorse correlate nella valutazione			
Hardware			
terminale x (id)			
Software			

Stima probabilità della minaccia *(motivata con riferimenti precisi agli articoli o ricerche sulle tendenze in corso) 1=inferi*

Minaccia	m_ris	m_int	m_disp	prob_m
ex: danneggiamento apparecchiatura x (guasto hardware)	0	3	3	1

Motivazione sulle stime

Il guasto di un terminale non incide sulla riservatezza dell'asset ma incide massimamente sull'integrità e disponibilità del dato se non sono previsti backup

Minaccia	m_ris	m_int	m_disp	prob_m

Motivazione

Minaccia	m_ris	m_int	m_disp	prob_m

Motivazione

Minaccia	m_ris	m_int	m_disp	prob_m

Motivazione

Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**

Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				

Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				

Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				
Minaccia	**m_ris**	**m_int**	**m_disp**	**prob_m**
Motivazione				

Osservazioni:

Calcolo del rischio intrinseco

Formula R(m,a) = max { p(m) * z(m) * z(a) } con z= (z_ris, z_disp, z_int). Ad esempio, se p(m)=2, z(m) =(0,1,1), z(a) = (2,2,3) R_i(a)= max {(2*0*2),(2*1*2), (2*1*3) } = max (0,4,6) = 6 . Tale calcolo verrà ripetuto per ogni risorsa correlata al trattamento e come rischio intrinseco del trattamento verrà considerato il valore massimo. **Basso rischio intrinseco = 0-6 Medio rischio intrinseco 7-12 Alto rischio intrinseco = 13-27 (tenere traccia della risorsa con il livello di rischio più alto).**

Punteggio di vulnerabilità *(assegnato in seguito a valutazione globale dei due audit)* ***3=controllo sotto alla media 2= controllo nella media 1= controllo oltre la media.***

necessario un trattamento se > 36

Asset	Rischio intrinseco	Vulnerabilità	Rischio totale (R*V)

Risk Assessment - Ponderazione del rischio
Questa scheda prende in input il livello di rischio totale del trattamento sui diritti degli interessati determinato in fase di analisi e ottiene in output una **valutazione di accettabilità o di trattamento del rischio**

Criteri di ponderazione
I criteri di accettabilità sono quelli che bilanciano il rischio di impresa e la sua sostenibilità in termini economici. Il trattamento del rischio consiste in una serie di misure mirate ad abbassare il valore della ***p(m)*** oppure i parametri di impatto ***a_int*** , ***a_disp*** dell'asset oggetto del trattamento. Potrebbe accadere che il Responsabile dei Dati (DPO) ritenga necessarie dette misure per contenere il livello di rischio individuato. Il Titolare del trattamento può decidere di non eseguire queste disposizioni motivando opportunamente tale scelta, ad esempio perchè non sostenibili economicamente.

Trattamento del rischio	
Dati del DPO	
Responsabile dell'esecuzione delle misure	
Prossimo controllo pianificato il	
Politica della sicurezza delle informazioni	
Organizzazione della sicurezza delle informazioni	

La gestione degli asset
La gestione dei supporti
Controllo degli accessi

Crittografia
Sicurezza fisica e ambientale
Sicurezza delle apparecchiature

Sicurezza delle attività operative
Malware
Backup
Raccolta di log e monitoraggio

Controllo del software di produzione
Gestione delle vulnerabilità tecniche
Gestione della sicurezza della rete
Gestione della sicurezza del trasferimento delle informazioni
Gestione della sicurezza dei processi di sviluppo e supporto al trattamento

Gestione della sicurezza dei dati di test
Gestione della sicurezza delle informazioni nei rapporti con i fornitori
Gestione degli incidenti

Gestione della continuità
Gestione delle ridondanze
Gestione della conformità ai requisiti normativi

Registro dei Trattamenti

Dati del Titolare del Trattamento

Modalità di conservazione del Registro

Soggetti che hanno accesso al Registro

Nome	Cognome	Ruolo	Privilegi

Gestione revisione e aggirnamento

Responsabile della conservazione del registro e della sua revisione/aggiornamento

La revisione del registro è prevista con periodicità

Osservazioni

Il Titolare **Il Responsabile dei Dati**

Registro dei trattamenti

Nome del trattamento

l'art 4 GDPR definisce **trattamento**: qualsiasi operazione compiuta su dati personali, come *raccolta, organizzazione,registrazione,strutturazione,conservazione,adattamento, modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione, cancellazione*

Dati del Titolare del Trattamento

Descrizione funzionale

(descrizione dell'elaborazione, la sua natura, la portata, il contesto, gli scopi e le poste in gioco - nel senso dei benefici attesi)

Finalità esplicite e legittime

(art 5.1 b)

Dati utilizzati

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)?

Categoria di interessato

Base giuridica e liceità del trattamento

(art 6)

Durata *(art 5 e, periodo di conservazione limitato)*		
Qualità dei dati e principio di minimizzazione *(art 5 c)*		
Individuazione dei Responsabili del trattamento *(art 28 - identificati e regolati da un contratto)*		
Il Responsabile della Protezione dei dati è:		
Trasferimento dati a paesi extra UE *(ex art 44 GDPR ammesso solo se garantito adeguato livello di protezione o in base ad una decisione di adeguatezza (art 45)*	si	no
(art 14)	si	no
Comunicazione dei dati a terzi *(necessità di informativa art 13)*	si	no
I rischi per la libertà e i diritti degli interessati sono stati individuati e gestiti *(con le schede di privacy audit e security audit ed eventuale ponderazione /trattamento del rischio)*	si	no

Indicare eventuale adesioni del Titolare ad un Codice di Condotta o ad un Sistema di Certificazione *(se esistono descrivere in che modo contribuiscano a minimizzare i rischi)*	si no
Riepilogo risultato dell' analisi del rischio ed eventuali considerazioni sul piabno del trattamento	

Gestione degli incidenti

Evento	Data ora	Segnalato al Garante il	Misure intraprese