REGIONE TOSCANA
Giunta Regionale

Data Protection Policy – Addendum

Indicazioni tecnico-operative

1. Indice

1. Scopo del documento....4

2. Premessa....4

3. Elenco Documenti....4

Ispezione dell'Autorità Garante....6

1 Scopo del documento....6
2 Premessa....6
3 Il Garante e i poteri allo stesso attribuiti a norma del GDPR....6
4 Il calendario delle ispezioni....9
5 Il protocollo d'intesa tra Garante e Guardia di Finanza....10
6 La gestione delle ispezioni....10
7 Riconoscimento degli ispettori ed accesso ai locali....11
8 Limiti dell'ispezione....11
9 Svolgimento dell'ispezione....11
9.1 Orari e preavviso....11
9.2 Attività e richieste informative e documentali....12
9.3 Suggerimenti per il Titolare nel corso di un'ispezione....12
9.4 Conclusione dell'ispezione....12
9.5 Suggerimenti....13
10 Conclusioni e indicazioni organizzative....13

Procedure di acquisto di servizi IT....15

1 Scopo del documento....16
2 Premessa....16
3 Procedure di acquisto....16
3.1 Documenti aggiuntivi per la Data Protection....17
3.2 Norme Contrattuali....19

Attività di controllo sui fornitori IT....20

1 Scopo del documento....21
2 Premessa....21
3 Analisi preliminare della fornitura IT....21
4 La Titolarità del trattamento....22
5 La contrattualizzazione dei doveri del Responsabile del trattamento....22
6 Quando svolgere gli audit....23
7 Modalità di svolgimento degli audit....23
8 L'audit report e il remediation plan....24
9 Riepilogo dei controlli....24
9.1 Controlli formali....24
9.2 Controlli di merito....27

Accordo fra Fornitori....30

1 Scopo....31
2 Premessa....31
3 Schema DPA P2P....32
3.1 Oggetto dell'accordo....32
3.2 Valutazione della rilevanza dei dati trattati....32

3.3 Descrizione del sistema....32
3.4 Impegni e ruoli ai fini della protezione dei dati....33
3.5 Descrizione delle componenti del sistema complessivo....33
3.6 Organizzazione per la sicurezza....33
3.7 Dichiarazione congiunta sulla adeguatezza a norma GDPR delle misure adottate....34

Misure di sicurezza e loro classificazione....35
1 Scopo....36
2 Premessa....36
3 Valore del dato....36
3.1 TIPOLOGIA DI DATO PERSONALE....36
3.2 CATEGORIE INTERESSATI....37
3.3 NUMERO DI PERSONE COINVOLTE NEL TRATTAMENTO....37
4 Misure di sicurezza aggiuntive per i trattamenti di dati personali....37
4.1 Correlazione fra valore del dato e livelli di misure di sicurezza....38
5 Controlli e misure di sicurezza....41
5.1 Misure organizzative....41
5.2 Misure tecniche....41
5.3 Lo standard ISO/IEC 27701....44
5.4 NIST Privacy Overlay....47
6 Un Primo Passo....49
6.1 Disegno architetturale....49
7 Famiglie e controlli – primo step....51
7.1 Famiglia: Sicurezza delle identità....52
7.2 Famiglia: Sicurezza dei dispositivi di accesso....53
7.3 Famiglia: Sicurezza delle reti....55
7.4 Famiglia: Sicurezza dei Sistemi....55
8 Riferimenti....58

1 Scopo del documento

Il presente documento costituisce una integrazione e una specificazione della Data Protection Policy, con l'obiettivo di fornire ulteriori linee guida e strumenti utili, al continuo adeguamento dei processi produttivi dell'ente, finalizzati al rispetto della normativa europea e nazionale in materia di Protezione dei dati personali.

2 Premessa

L'esperienza di questo primo periodo di applicazione della Data Protection Policy ha messo in evidenza alcuni aspetti che necessitano di un migliore o maggiore approfondimento.
I documenti raccolti in questo Addendum alla Data Protection Policy, hanno come obiettivo quello di informare e guidare su aspetti particolari come ad esempio,

3 Elenco Documenti

Nella seguente tabella sono riportati: i titoli dei documenti che costituiscono questo addendum; la loro descrizione in termini di obiettivo che vogliono raggiungere e i destinatari a cui sono rivolti.

Titolo del documento	***Descrizione***	***Destinatari***
Ispezioni del Garante	L'obiettivo di questo documento è illustrare motivazioni e procedure seguite dal Garante nelle fasi ispettive e di fornire una linea guida di organizzazione e comportamento da tenere durante le diverse fasi dell'ispezione	Titolari e loro delegati, Data Protection Specialist, Security IT Manager, Ufficio del DPO, addetti alla sicurezza IT.
Procedure di acquisto servizi IT	L'obiettivo di questo documento è descrivere, limitatamente al tema Data Protection e in sintesi, i documenti da predisporre, come allegati, in una procedura di acquisto di servizi IT.	Dirigenti e tecnici che predispongono atti per acquisti di servizi IT, Ufficio Contratti, RUP e DEC di contratti di forniture di servizi IT, ai Responsabili
Controlli sui Fornitori di servizi IT	L'obiettivo di questo documento è fornire una linea guida sulle motivazioni e sulle procedure da seguire per effettuare attività di controllo (Audit) sui fornitori di servizi IT nominati Responsabili, da parte dei Titolari, attraverso i supporti organizzativi del proprio ente.	Titolari o loro delegati, Data Protection Specialist, Security IT Manager, Ufficio del DPO, Responsabili di contratto e Direttori Esecutivi dei Contratti (DEC).
Data Protection Agreement fra fornitori (DPA P2P)	L'obiettivo di questo documento è motivare l'esigenza di procedere a	Data Protection Specialist, dirigenti che eseguono procedure di acquisto di

	formalizzare un accordo fra Fornitori quando questi concorrono, attraverso contratti diversi, alla erogazione di un unico servizio.	forniture IT, RUP, DEC, Ufficio Contratti, Security IT Manager.
Valutazione dei dati personali e misure di sicurezza	L'obiettivo di questo documento è fornire una metodologia di valutazione del "valore dei dati" in termini di rischio potenziale per le libertà e i diritti degli interessati, e di correlare a tale valore dei livelli di sicurezza da adottare attraverso misure adeguate.	Data Protection Specialist, Security IT Manager, dirigente responsabile di contratti, RUP, DEC, Responsabili.

Ispezione dell'Autorità Garante

Norme di comportamento

1 Scopo del documento

Il presente documento ha lo scopo di fornire informazioni in relazione alle ispezioni che l'Autorità Garante per la protezione dei dati personali (nel prosieguo Garante), svolge ai fini della verifica del rispetto dei principi generali e degli adempimenti previsti dal Reg. UE n. 679/2016 (in seguito GDPR) e dal D. Lgs. n. 196/2003, come modificato dal D. Lgs. n. 101/2018 (in seguito anche D. Lgs. n. 196/2003).
L'obiettivo perseguito è, altresì, proporre indicazioni sui comportamenti più opportuni da assumere nel corso di un'ispezione.

2 Premessa

Le ispezioni del Garante possono attivarsi secondo una sua pianificazione o sulla base di richieste da parte degli interessati. L'ispezione è una attività che richiede la massima e trasparente collaborazione del soggetto, oggetto dell'ispezione stessa. Nessun impedimento deve essere frapposto all'attività del Garante; attività che richiede la piena e leale collaborazione al fine di individuare eventuali mancanze. Deve esistere solidale interesse sia del Titolare, in particolare in quanto ente pubblico, sia del Garante, nel processo di verifica, in quanto finalizzato alla tutela dei diritti e delle libertà dei cittadini e al pieno rispetto delle leggi.
Occorre sempre tenere presente i principi sanciti dal GDPR in merito alla tutela dei diritti degli interessati e l'obbligo in questo dell'Accountability, del saper rendere conto della propria attività, da parte del Titolare. Il Garante opera sempre ed esclusivamente a tutela degli interessati.

3 Il Garante e i poteri allo stesso attribuiti a norma del GDPR

Il "Garante" è un'autorità amministrativa indipendente istituita con la "cosiddetta" legge sulla privacy, L. n. 675/1996, poi disciplinata dal Codice in materia di protezione dei dati personali D. Lgs. n. 196/2003, come modificato dal D. Lgs. n. 101/2018.
Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del GDPR (art. 51).
All'interno dell'art. 58 del GDPR possono distinguersi 3 tipologie di poteri attribuiti al Garante:

1) **Poteri di indagine (comma 1):**
   a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
   b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
   c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
   d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;
   e) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri".
2) **Poteri correttivi (comma 2):**
   a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del regolamento;
   b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del regolamento;

c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal regolamento;
d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e
j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale".

3) **Poteri autorizzativi e consultivi** (comma 3):
a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36;
b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;
c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;
d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5;
e) accreditare gli organismi di certificazione a norma dell'articolo 43;
f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5;
g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);
i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b);
j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47".

Con riguardo alla prima categoria di poteri, quelli ispettivi, si rileva che il Garante ha la possibilità di richiedere che gli siano forniti informazioni o documenti, anche con riferimento a banche dati, sia al Titolare; sia al Responsabile, che all'Interessato ed ai Terzi (art. 157 D. Lgs. 196/2003).
Il Garante, inoltre, nello svolgimento dei propri accertamenti può accedere a (art. 158 D. Lgs. 196/2003, comma 1):

a) banche dati;
b) archivi;
c) luoghi in cui si svolge il trattamento o comunque utili al controllo.

Tali controlli possono essere effettuati anche per il tramite di:

a) personale dell'ufficio del Garante (art. 158 D. Lgs. n. 196/2003, comma 2);

b) altri organi dello Stato, se necessario (art. 158 D. Lgs. n. 196/2003, comma 3).

Qualora i predetti controlli debbano essere effettuati in luoghi di privata dimora (art. 158 D. Lgs. n. 196/2003, comma 4) sono necessari:

a) il consenso informato del Titolare o del Responsabile;
b) l'autorizzazione del Presidente del Tribunale territorialmente competente.

Si sottolinea che la falsità di informazioni e documenti forniti al Garante è sanzionata con la pena detentiva, ai sensi del D. Lgs n. 196/2003, art 168:

a) Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
b) Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno, chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti".

4 Il calendario delle ispezioni

Il Garante definisce, a cadenza semestrale, un programma di ispezioni da effettuare. La deliberazione con cui approva e rende noto il programma è pubblicata e disponibile per la consultazione all'interno del sito web del Garante; ivi, possono rinvenirsi gli ambiti e le aree specifiche che saranno oggetto di ispezione per il semestre in corso.

Si suggerisce pertanto di esaminare ogni semestre il calendario predisposto dal Garante.

A titolo esemplificativo all'interno del programma per il primo semestre 2020, tra le altre, le aree sottoposte ad ispezione sono:

a) trattamenti di dati personali effettuati da Enti pubblici relativamente alla c.d. medicina di iniziativa;
b) trattamenti di dati relativi alla salute effettuati da società multinazionali operanti nel settore farmaceutico e sanitario;
c) trattamento di dati personali effettuati nel quadro dei servizi bancari on line; trattamenti dei dati personali effettuati mediante applicativi per la gestione delle segnalazioni di condotte illecite (c.d. whistleblowing);
d) trattamenti dei dati personali effettuati da intermediari per la fatturazione elettronica; trattamenti di dati personali effettuati da Enti pubblici in tema di rilascio di certificati anagrafici e di stato civile, attraverso l'accesso ad ANPR;
e) trattamenti di dati personali effettuati da società private ed Enti pubblici per la gestione e la registrazione delle telefonate nell'ambito del servizio di call center;
f) trattamenti di dati personali effettuati da società per attività di marketing; trattamenti di dati personali effettuati da società con particolare riferimento all'attività di profilazione degli interessati che aderiscono a carte di fidelizzazione;
g) trattamenti di dati personali effettuati da società rientranti nel settore denominato "Food Delivery";
h) trattamento di dati personali effettuati da società private in tema di banche reputazionali;
i) data breach.

Si rimanda alla "Deliberazione del 6 febbraio 2020. Attività ispettiva di iniziativa curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio giugno 2020 [9269607]" per visionare il calendario completo del primo semestre 2020.

5 Il protocollo d'intesa tra Garante e Guardia di Finanza

Come sopra già indicato (si veda par. 3), l'art. 158, comma 3, del D. Lgs. n. 196/2003 stabilisce che, per lo svolgimento delle sue funzioni, l'Autorità Garante per la protezione dei dati personali si avvale, ove necessario, anche della collaborazione di altri organi dello Stato.
Nell'ambito di questo quadro normativo ed in attuazione dei principi contenuti nel D. Lgs. n. 68/2001, il Presidente dell'Autorità Garante ed il Comandante Generale pro tempore della Guardia di Finanza, hanno sottoscritto, il 10 marzo 2016, un Protocollo d'Intesa che ribadisce la competenza generale del Corpo in materia economico-finanziaria e ne prevede espressamente la collaborazione con le Autorità indipendenti.
Il Garante ha attivato il *Nucleo Speciale Tutela Privacy e Frodi Tecnologiche*, quale Reparto della Guardia di Finanza individuato per assicurare, su tutto il territorio nazionale o previo interessamento del Reparto territorialmente competente, gli adempimenti connessi all'attività di collaborazione.
Lo scopo del protocollo è assicurare all'Autorità, tramite l'Unità Speciale, un'efficace collaborazione nello svolgimento delle sue funzioni ispettive, conoscitive e informative sui fenomeni che riguardano il trattamento dei dati personali.
In particolare, il Corpo collabora all'attività ispettiva condotta dal Garante attraverso:

a) il reperimento di dati e informazioni sui soggetti da controllare;
b) la partecipazione di proprio personale agli accessi alle banche dati, ispezioni, verifiche e alle altre rilevazioni nei luoghi ove si svolge il trattamento;
c) l'assistenza nei rapporti con le Autorità Giudiziarie;
d) lo sviluppo delle attività delegate o sub-delegate per l'accertamento delle violazioni di natura penale o amministrativa;
e) la contestazione delle sanzioni amministrative rilevate nell'ambito delle attività delegate;
f) la partecipazione, a richiesta del Garante, a ispezioni congiunte con autorità di protezione dei dati personali di altri Paesi;
g) l'esecuzione di indagini conoscitive sullo stato di attuazione della legge in settori specifici;
h) l'esecuzione di verifiche online volte a rilevare, dall'esame di siti web, il rispetto della normativa;
i) la progettazione e l'attuazione d'intesa con il Garante, di altre iniziative anche nell'ambito delle cooperazioni internazionali.

Con il Protocollo d'Intesa, inoltre, sono state previste più strette sinergie nell'attività di informazione in tema di protezione dei dati personali, mediante il supporto dell'Autorità nei processi di formazione del personale in materia di protezione dei dati personali.

Il Garante, conformemente al Protocollo d'Intesa, invia delle specifiche richieste di collaborazione alla Guardia di Finanza (art. 3 Protocollo d'Intesa), che devono contenere gli elementi seguenti:

a) Ambito;
b) Scopo dell'intervento;
c) Soggetti interessati;
d) Enunciazione dei fatti e delle circostanze;
e) Modalità con le quali è chiesto di reperire i dati e le informazioni, di fornire assistenza, di partecipare all'esecuzione di ispezioni ecc.

6 La gestione delle ispezioni

Durante una visita ispettiva da parte del Garante gli attori coinvolti sono ascrivibili essenzialmente a due parti:

1) Ispettori, che come sopra descritto potranno essere soggetti afferenti all'Ufficio del Garante e/o alla Guardia di Finanza, nucleo speciale privacy;
2) Titolare (o eventualmente Responsabile) che è opportuno si strutturi in modo adeguato ad accogliere le eventuali ispezioni con:
   a) un Comitato di accoglienza (per garantire un clima collaborativo tra ispettori e Titolare, agevolare l'accesso ai locali e la comunicazione con i soggetti che saranno tenuti a fornire le informazioni e la documentazione richiesta);
   b) il gruppo che si occupa della protezione dei dati personali (nel caso della Giunta Regionale sarà composto dai delegati del Titolare e dai Data Protection Specialist delle Direzioni coinvolte nell'ispezione, nonché da ulteriori autorizzati nei trattamenti ispezionati);
   c) il Data Protection Officer ed il suo ufficio (DPO e i dipendenti del suo ufficio, che nel caso degli enti regionali coincidono con i Data Protection specialists);
   d) i Responsabili/Dirigenti dei processi sottoposti ad ispezione;
   e) i consulenti esterni, che collaborano con il DPO ed il suo Ufficio, da cui il Titolare può chiedere di essere assistito durante l'ispezione.

7 Riconoscimento degli ispettori ed accesso ai locali

Gli ispettori incaricati di svolgere l'accertamento, si dovranno far riconoscere tramite esibizione di un documento di riconoscimento che ne attesti formalmente il ruolo.
Per l'accesso ai locali, inoltre, gli ispettori dovranno essere muniti di un incarico formale da parte del Garante.
Nel predetto documento denominato "ordine di servizio" devono risultare:

a) Titolare (o Responsabile) soggetti all'ispezione;
b) Tipologia di poteri di indagine utilizzati nell'ispezione;
c) Ambito del controllo;
d) Luogo ove si svolge l'accertamento;
e) Responsabile dell'attività ispettiva e ulteriori partecipanti;
f) Designati d'intesa con i dirigenti dei dipartimenti, servizi o altre unità organizzative;
g) Sanzioni previste.

Per l'accesso ai locali di privata dimora l'art. 158 D. Lgs. n. 196/2003, comma 4, richiede:

a) il consenso informato del Titolare o del Responsabile;
b) l'autorizzazione del Presidente del Tribunale territorialmente competente.

8 Limiti dell'ispezione

Vi è un limite dell'ispezione connesso alla materia verificata; nello specifico se la Guardia di Finanza sta effettuando un controllo in materia fiscale, non può effettuare anche un controllo sulla protezione dei dati personali.
In una simile ipotesi il Protocollo d'Intesa tra Garante e Guardia di Finanza prevede che quest'ultima segnali al Garante le situazioni rilevanti in ambito protezione dei dati personali, di cui sia venuta a conoscenza nel corso dello svolgimento del proprio servizio; sarà poi il Garante a valutare la segnalazione ricevuta e qualora lo ritenga opportuno a predisporre l'avvio di un'attività di accertamento sul tema, eventualmente incaricando la Guardia di Finanza per un'ispezione e predisponendo un ordine di servizio, come sopra dettagliato.

9 Svolgimento dell'ispezione

9.1 Orari e preavviso

“Gli accertamenti, se effettuati presso il Titolare o il Responsabile, sono eseguiti dandone informazione a quest’ultimo, se questi è assente o non è designato, agli incaricati “ (art. 159 del D. Lgs. n. 196/2003, comma 3).
Per quanto attiene l’orario di svolgimento delle ispezioni ed il preavviso delle stesse, salvo che sia disposto diversamente nel decreto di autorizzazione del presidente del tribunale, l’accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso, quando ciò può facilitarne l’esecuzione (art. 159 del D. Lgs. n. 196/2003, comma 4).
In sostanza l’orario di inizio delle ispezioni è tra le ore 7:00 e le ore 20:00 e queste possono essere svolte senza o con preavviso; che viene dato nel caso possa semplificare il controllo da svolgere.
Nella pratica è accaduto più frequentemente che le ispezioni rientranti nell’ambito dei piani/programmi semestrali del Garante non siano state annunciate, mentre le altre generalmente sono preannunciate.

9.2 Attività e richieste informative e documentali

Le attività dell’ispezione, indicativamente, possono occupare lo spazio temporale di 3 (tre) giornate e principalmente consistono in:

a) Raccolta della documentazione;
b) Approfondimento degli aspetti generali (es. nomina DPO, modello organizzativo, ecc..), attraverso sia un’analisi dei documenti che tramite interviste dirette;
c) Approfondimento di aspetti specifici, connessi all’ambito ispezionato (interviste con i responsabili di processo coinvolti; simulazione di casi pratici (es. iscrizione sito e-commerce); accesso ai sistemi con screenshot delle operazioni; estrazione e confronto dei dati estratti dai sistemi informativi.

Si sottolinea che solitamente la verifica del Registro dei Trattamenti è il punto di partenza delle ispezioni svolte.

Nel caso in cui al momento dell’ispezione i documenti richiesti non siano disponibili possono essere forniti al Garante in un momento successivo e congruo, generalmente non superiore a 30 giorni.

9.3 Suggerimenti per il Titolare nel corso di un’ispezione

Dal punto di vista pratico, i comportamenti che seguono sono molto utili:

a) Annotare i documenti che sono visionati dagli ispettori e le informazioni richieste e fornite nel corso dell’ispezione;
b) Consegnare copie conformi della documentazione richiesta e conservare gli originali;
c) Mantenere un comportamento collaborativo nei confronti del personale che svolge l’ispezione;
d) Chiedere una copia del verbale che viene redatto dagli ispettori.

*Si sottolinea, inoltre, che il Titolare **deve garantire di avere conoscenza chiara** di tutte le logiche e dinamiche contrattuali di cui è parte **(soprattutto in ambito misure di sicurezza)** e quindi nei rapporti con i soggetti esterni nominati Responsabili cui sono affidati specifici servizi in ambito trattamento dati personali.*
L’importanza di ciò è avvalorata dal fatto che talvolta il Garante, in ispezioni svolte, ha escluso la possibilità di coinvolgimento di altri soggetti, sulla base dell’assunto che il Titolare, “Controller”, deve avere un controllo e conoscenza completa (documentale non necessariamente tecnica) anche delle attività affidate ad altri soggetti terzi esterni.

9.4 Conclusione dell’ispezione

Al termine dell’attività ispettiva gli output del Garante possono essere i seguenti:

a) Verbale firmato da tutte le parti;

b) Richiesta di integrazione;
c) Istruttoria di 3 mesi con ordinanza in 5 anni;
d) Richiami; Misure Correttive; Blocco del trattamento; Sanzioni amministrative.

9.5 Suggerimenti

I comportamenti che in linea di massima devono essere tenuti nel corso di un'ispezione per garantirne il corretto svolgimento possono riassumersi come segue:

a) Garantire il coinvolgimento delle figure apicali dell'organizzazione (es. Dirigenti, Direttori ecc.);
b) Avere un gruppo composto: da competenze legali, di Innovation Tecnology (IT) o archivistiche (dipendendo dai mezzi di trattamento dati), data la trasversalità del tema della protezione dei dati personali;
c) Avere il Registro dei Trattamenti completo e aggiornato;
d) Avere sempre a disposizione per ogni trattamento, i documenti che verrebbero richiesti in un'ispezione (DPA, eventuale DPIA ecc…);
e) Formalizzare le scelte effettuate ed avere a disposizione i verbali che le attestano (se si adottano scelte rischiose si potrebbe essere chiamati a dimostrarne la legittimità);
f) Formalizzare le attività svolte dal DPO (Linee giuda, monitoraggio, ecc…);
g) Effettuare simulazioni di attività ispettive (documentare con report);
h) Collaborare con l'autorità Garante e dire la verità.

10 Conclusioni e indicazioni organizzative

Ai fini del rapporto con il Garante sono essenziali gli elementi richiamati dal principio di accountability fortemente introdotto dal GDPR. Tale principio richiede leale collaborazione, trasparenza, documentazione aggiornata attestante l'attenzione prestata al tema della Data Protection in tutte le fasi di attivazione e gestione di processi che coinvolgono il trattamento di dati personali (Data Protection by Design, by Default).
Essenzialmente un'ispezione si compone di due fasi, una documentale e l'altra ispettiva vera e propria.
Per il primo punto disporre della documentazione e fornirla il più completa possibile nel minor tempo possibile è un elemento di estrema importanza, in quanto denota attenzione, controllo e conoscenza delle problematiche trattate e concreta volontà di agevolare e non contrastare l'azione ispettiva.
Per la seconda avere un protocollo chiaro di collaborazione con l'ufficio del Garante a dimostrazione della volontà di non nascondere nulla e di condividere in trasparenza problemi riscontrati (incidenti) e soluzioni attuate, è fondamentale per dimostrare che non c'è stata sottovalutazione dei problemi e che si sono attivate tutte le azioni necessarie a minimizzare il danno nell'immediato e a mettere in campo soluzioni atte al non verificarsi più di tali problemi.
Al fine di assistere il Titolare, al momento della ispezione, viene costituito un ***gruppo di lavoro*** composto:

a) Dal titolare stesso che lo coordina;
b) Dal DPO;
c) Dal Security IT Manager;
d) Dai Data Protection Specialist coinvolti.

*La documentazione da fornire **nell'immediato** riguarda:*

1) L'organizzazione dell'Ente (delibere, documenti, certificazioni, ecc..);
2) Le attività del DPO a testimonianza dello svolgimento dei sui compiti di consulenza e sorveglianza (linee guida, indirizzi, monitoraggio, verifiche, formazione, ecc..);

3) Il registro dei trattamenti (formato PDF mensile);
4) Per il/i trattamenti oggetto della richiesta di ispezione:
    a. I contratti/convenzioni con altri soggetti;
    b. Data Protection Agreement collegati ai contratti del punto precedente, nel quale si formalizzano le nomine degli altri soggetti secondo i ruoli GDPR, si descrivono le tipologie dei dati e delle categorie degli interessati e le relative misure di sicurezza;
    c. Eventuale Data Protection Impact Assessement (DPIA);
    d. Report sintetico degli incidenti occorsi;
    e. L'elenco degli amministratori di sistema.

Tali documenti sono organizzati in cartelle digitali a cura dei Data Protection Specialist e la loro collocazione in digitale (cartelle di rete, web, piattaforma di collaboration, sistema documentale), è opportuno sia comunicata all'ufficio del DPO. *(Questo data l'attuale situazione in cui Regione Toscana non dispone di un sistema documentale condiviso)*

*Su richiesta dovranno essere forniti **nel più breve tempo** possibile:*

1) Documenti tecnici attestanti le misure di sicurezza effettivamente attivate per i trattamenti oggetto di ispezione,
2) gli incidenti occorsi e i remediation plan attivati,
3) motivazioni tecniche e organizzative, qualora non esista una DPIA, che dimostrino l'adeguatezza delle misure di sicurezza adottate,
4) le attività di audit svolte dal Titolare sul Responsabile a dimostrazione dell'esercizio della sua funzione di controller,
5) eventuali credenziali per l'accesso al registro dei trattamenti e ai sistemi e alle procedure,
6) ogni altro documento che il Garante richiederà.

Al fine di rispondere a richieste tecniche specifiche del Garante e per assisterlo in maniera efficiente ed efficace nelle ispezioni in loco, al momento della ispezione è opportuno che si formalizzi la costituzione di un ***team tecnico*** coordinato dal Security IT Manager e composto:

a) Dal Security IT Manager,
b) dal titolare o suo delegato,
c) dal/i Data Protection Specialist,
d) da un rappresentante dell'ufficio del DPO,
e) dal responsabile (se coinvolto) insieme al relativo DPO e responsabile della sicurezza.

Procedure di acquisto di servizi IT
Linee Guida

1 Scopo del documento

Questo documento ha come obiettivo quello di evidenziare, nel rispetto del principio, sancito dal GDPR, Data Protection by Design, i documenti aggiuntivi necessari in fase di predisposizione del bando di gara o di altre procedure per effettuare l'acquisto di servizi digitali (servizi IT). Qualora questi documenti non fossero predisposti in fase di gara ed essere oggetto di valutazione nel processo di aggiudicazione e contrattualizzazione, occorre che si proceda alla loro formalizzazione nelle fasi immediatamente successive, avendo ben presente che questo potrà comportare attività aggiuntive e/o ulteriori problemi e complicazioni di varia natura.

2 Premessa

L'approvazione del documento Data Protection Policy (DPP), da parte di tutti gli Enti del sistema regionale, ha costituito un primo importante passo di inquadramento delle attività di ciascuno nel pieno rispetto della normativa sulla Protezione dei Dati. Nel documento della DPP sono elencati tuti gli adempimenti necessari alla compliance con il GDPR e sono forniti tutti i modelli di contratti (DPA) da sottoscrivere con i fornitori di servizi IT, nelle diverse fattispecie di relazioni Titolare-Responsabile, Titolare-Titolare, Contitolari e sono fornite indicazioni di carattere generale in merito al processo di acquisizione di servizi che prevedono il trattamento di dati personali.
In questo documento si andrà pertanto ad elencare e motivare i soli documenti aggiuntivi da prevedere nel capitolato di gara ed il loro utilizzo nelle successive fasi di contrattualizzazione e conduzione dei contratti di servizi IT che prevedono il trattamento di dati personali.

Per semplificazione si ritiene utile rappresentare un sistema informativo come un insieme di trattamenti dati, denominati servizi IT applicativi (applicazioni) che si appoggiano, per la loro , dei servizi IT infrastrutturali (server, reti, DBMS, ecc..).
In sintesi una componente applicativa e una componente infrastrutturale di tipo tecnologico.

3 Procedure di acquisto

Una ***"procedura di acquisto"*** (con questo termine intendiamo qualsivoglia procedura di acquisto, bando di gara, ordine diretto, ecc..) può prevedere l'acquisizione delle seguenti tipologie di servizi:

1) Acquisto dei servizi IT applicativi (applicazioni), prevedendo l'utilizzo di infrastrutture:
   a) già disponibili tramite un contratto con altro fornitore,
   b) già disponibili a gestione diretta dell'ente;
2) Acquisto di Servizi IT infrastrutturali (in sigla IaaS, PaaS) su cui appoggiare:
   a) servizi applicativi acquisiti tramite altro contratto con altro fornitore,
   b) servizi applicativi gestiti sotto la responsabilità di strutture organizzative dell'ente;
3) Acquisto di servizi applicativi e infrastrutturali da un unico fornitor, comprensivi della tipologia SaaS (servizi applicativi in Cloud).

In più occorre ricordare che le procedure di acquisto possono prevedere come "***offerenti":***

1) Un'unica figura giuridica;
2) Un raggruppamento temporaneo di impresa (RTI, ATI, ecc..) composto da più soggetti con figure giuridiche diverse.

Queste diverse tipologie di obiettivi a cui vengono finalizzate le procedure di acquisto, saranno riprese successivamente andando ed evidenziare cosa cambia nel rapporto Cliente - Fornitore/i, così come occorra tenere presente se siamo in presenta di un RTI o meno.
Le ***figure organizzative*** coinvolte nella fase di ***predisposizione delle "procedure di acquisto" del tipo 1) e 3)*** sopra illustrate, sono:

1) Il responsabile/i (dirigente) del settore/i competente nella materia oggetto del sistema informativo. Per il trattamento dei dati personali tale responsabile coincide con il Titolare dei trattamenti o suo delegato;
2) Il responsabile dei sistemi informativi dell'ente e dal responsabile delle infrastrutture se coinvolto;
3) Personale tecnico delle strutture coinvolte utili alla predisposizione dei documenti di gara;
4) Personale dell'ufficio contratti.

Le ***figure organizzative*** coinvolte nella fase di ***predisposizione delle "procedure di acquisto" del tipo 2)*** sopra illustrate, sono:

1) Il responsabile delle infrastrutture e il responsabile dei sistemi informativi se coinvolto;
2) Personale tecnico delle strutture coinvolte, utili alla predisposizione dei documenti di gara;
3) Ufficio contratti.

Le figure organizzative coinvolte nella ***conduzione del contratto:***

1) Il responsabile del contratto;
2) Il Responsabile Unico del Procedimento;
3) Il Direttore Esecutivo del Contratto;
4) Il Fornitore.

3.1 Documenti aggiuntivi per la Data Protection

Di seguito si elencano i documenti necessari da predisporre all'interno delle procedure di acquisto finalizzati al rispetto del principio di Data Protection by Design by Default del GDPR. Tali documenti si vanno ad aggiungere o ad integrare agli altri già presenti e normalmente utilizzati.
I documenti sono suddivisibili in:

1) Documenti illustrativi, finalizzati a fornire delle specifiche (requirements),
2) Modelli di documenti che il partecipante alla procedura deve compilare come parte integrante dell'offerta,
3) Documenti prescrittivi laddove esistenti.

3.1.1. Scheda Data Protection

La *scheda Data Protection* da prevedere per le **procedure di acquisto di tipo 1) e 3)** che coinvolgono l'acquisizione di applicazioni IT deve, sulla base del documento, ***"Valutazione e misure della sicurezza" "sezione valutazione dei dati trattati***", descrivere :

1) I trattamenti,
   a) il valore dei dati trattati sulla base dei parametri relativi alla tipologia dei dati, alle categorie degli interessati e alla numerosità degli stessi,
      i) il livello delle misure di sicurezza da adottare (bassa, media, alta) considerando in questo dati sanitari e giudiziari.

La compilazione di detta schedaè a carico del dirigente competente per materia (Titolare), coadiuvato dal Data Protection Specialist o dall'ufficio del DPO.

3.1.2. Scheda misure di sicurezza

Tale scheda riguarda tutte le tipologie di procedure di acquisto ed è composta da due sezioni, (i) misure di sicurezza delle applicazioni, (ii) misure di sicurezza infrastrutture, ds compilaer sulla base della tipologia dei servizi offerti.

La prima sezione dovrà essere compilata dall'offerente nelle procedure di tipo 1),
La seconda sezione dovrà essere compilata dall'offerente nelle procedure di tipo 2),
La prima e la seconda insieme dovranno essere compilate dall'offerente nelle procedure di tipo 3).

La scheda Data Protection e la scheda delle misure di sicurezza devono essere viste come una unica scheda redatta secondo lo schema e le valutazioni riportate nel documento "Valutazioni e misure di sicurezza". La non compilazione della scheda misure di sicurezza da parte del partecipante deve essere considerato motivo di esclusione dalla procedura di acquisto e deve essere previsto, nell'ambito del processo di valutazione dell'offerta tecnica, un adeguato punteggio relativo alle misure di sicurezza proposte.

NOTA BENE: *Nel caso di infrastrutture IT complesse e predisposte per accogliere in modo trasversale, diversi sistemi informativi, deve essere previsto nella scheda delle misure di sicurezza, un disegno architetturale che consenta in modo semplice di individuare ambiti infrastrutturali e ambienti e soluzioni che possano configurare strutturalmente:*
aree pubbliche, aree con misure di sicurezza bassa, media e alta con considerazioni in riferimento ai dati sanitari e giudiziari.

3.1.3. Scheda Data Protection Agreement (T-R/T-T)

Al Bando di gara o ad altro atto di inizio della procedura di acquisto deve essere allegato, o deve fare parte integrante della proposta di Contratto, se presente, lo schema di Data Protection Agreement: compilato per la parte relativa all'ente, utilizzando le informazioni già presenti nella "Scheda Data Protection" ed essere compilato, dall'offerente, per le parti di sua competenza con particolare riferimento alle misure di sicurezza adottate così come descritte nel modello "Scheda misure di sicurezza". Il Data Protection Agreement compilato e firmato deve far parte della documentazione prodotta dall'offerente in fase di offerta, pena la esclusione dalla gara.

3.1.4. Scheda Data Protection Agreement fra fornitori (DPA P2P)

Qualora ci si ritrovi nelle condizioni di procedure di acquisto del tipo 1.a) o 2.a), che prevedono l'interazione dell'offerente con altro fornitore che assicura servizi infrastrutturali o servizi applicativi, rispettivamente, deve essere allegato l'ulteriore schema Data Protection Agreement (DPA P2P) che l'offerente si deve impegnare ad adottare entro un tempo prefissato (es. 30 giorni dalla firma del contratto o inizio della fornitura) a discrezione del responsabile del contratto.
Si ricorda che qualora il Titolare non ritenesse necessario un accordo fra i diversi fornitori che congiuntamente si impegnano a garantire il corretto trattamento di dati personali e l'efficiente supporto congiunto al Titolare stesso, ricade esclusivamente sotto la sua responsabilità diretta il garantire la sicurezza complessiva del sistema informativo e il rispetto dei principi e delle regole della normativa europea e nazionale in materia di data protection.

3.1.5. Scheda Piano di qualità della fornitura

L'offerente deve obbligatoriamente, pena esclusione dalla procedura di acquisto, allegare all'offerta un "Piano di qualità della fornitura" che oltre ad altri elementi che il responsabile del contratto riterrà che debbano essere contemplati, deve contenere le informazioni riportate nella "Scheda Piano di Qualità della fornitura" che l'ente ha comunicato nell'ambito dell'avvio della procedura di acquisto.
In fase di valutazione dell'offerta deve essere previsto uno specifico punteggio relativo al livello di

qualità del Piano presentato. L'assenza della comunicazione del piano di qualità da parte dell'offerente deve essere considerato elemento invalidante l'offerta.

3.2 Norme Contrattuali

Qualora si sia nella condizione nella quale l'offerente non si configuri come una unica figura giuridica ma come un insieme di soggetti, che partecipano in raggruppamento temporaneo di impresa od altra forma prevista nella procedura di acquisto, occorre prevedere una delle opzioni seguenti:
1) Si fa obbligo che le mandanti nella procura di rappresentanza per gli aspetti contrattuali alla mandataria (capo gruppo), indichino anche la rappresentanza unitaria per tutti gli aspetti relativi ai compiti derivanti dalla normativa in materia di protezione dei dati personali. In questo caso la (Titolare) e gli altri partecipanti si configureranno come altri responsabili a norma del GDPR;
2) Si fa obbligo che i componenti il raggruppamento di imprese stipulino fra di loro un Data Protection Agreement del tipo P2P (DPA P2P);
3) Qualora non si attivi quanto previsto ai precedenti due punti, ricade sul Titolare garantire direttamente la sicurezza complessiva delle azioni e del coordinamento dei diversi soggetti con i quali avrà stipulato separati Data Protection Agreement.
Il principio ispiratore è che nello sviluppo e conduzione di un sistema informativo che tratta dati personali, si realizzi, attraverso impegni chiari ed espliciti, un rapporto solidale e di fiducia (Trust) fra il Titolare e i Responsabili che con ruoli diversi sono coinvolti nel garantire il sistema, applicativo e infrastrutturale, nel suo complesso.
Si invita inoltre a prevedere nel capitolato di gara e nel successivo contratto un importo, percentuale sul totale della fornitura, da dedicare all'obiettivo di migliorare o rendere adeguate le misure di sicurezza al mutare, nel periodo contrattuale, del contesto tecnologico e organizzativo inziale per il quale sono state ritenute adeguate le misure di sicurezza contrattualizzate.
Nel seguito del presente documento sono riportate le schede indicate.

Attività di controllo sui fornitori IT
Linee Guida

1 Scopo del documento

Lo scopo del presente documento è quello di fornire delle linee guida per la definizione dei controlli da effettuare nei confronti del Responsabile da parte del Titolare, nel caso specifico di fornitori di servizi IT o di altri soggetti che si configurano in tale ruolo.

2 Premessa

Nel caso di utilizzo di sistemi di Information Tecnology (IT) il Titolare può avvalersi di strutture interne alla propria organizzazione, di fornitori esterni attraverso specifici contratti di fornitura, di altri enti o soggetti nell'ambito di convenzioni. In ognuno di questi casi il Titolare, sia esso la Giunta regionale o un ente dipendente, è tenuto a svolgere la sua funzione di controllo in merito al puntuale rispetto, da parte del Responsabile, delle misure e delle procedure di sicurezza adottate.

Quindi premessa fondamentale è che nel rapporto Titolare Fornitore siano esplicitate nel Data Protection Agreement le misure di sicurezza adottate in relazione al "valore dei dati trattati".

Qualora i Responsabili siano fornitori, essi saranno soggetti, a cura del Titolare, a degli audit periodici (ai sensi dell'art. 28 comma 1 lett. H del GDPR), finalizzati a verificare il rispetto dell'agreement sottoscritto e al permanere della sua valenza.
Nel caso della Giunta regionale toscana e degli enti che si avvalgono della stessa struttura di Security IT Manager, i controlli sono ad essa demandati nell'ambito del piano annuale che deve predisporre (vedi Data Protection Policy). Rimane comunque in carico al Titolare verificare che i controlli siano pianificati, eseguiti e che siano stati individuati eventuali problemi e pianificati gli interventi di miglioramento ritenuti necessari.

3 Analisi preliminare della fornitura IT

Gli aspetti di rilievo in ambito GDPR, che emergono in relazione alla fornitura di servizi IT appaltata presso outsorcers, sono di duplice natura e si sviluppano su due piani.

Sul piano **soggettivo**, individuando i ruoli "Data Protection" da attribuire:
In prima istanza, andrà stabilito se il fornitore andrà o meno identificato nel ruolo di responsabile del trattamento (ovvero, in linea teorica, se sia identificabile come titolare autonomo o contitolare del trattamento). Tale ricorrenza sussiste se il fornitore è incaricato di effettuare uno o più trattamenti (art. 4, comma 1 nr. 2 GDPR: *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;"*) ricompresi nella definizione *ex* art. 4 comma 1 nr. 8 *("la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"*) per conto della Regione Toscana, quale titolare del trattamento.
Per identificare correttamente la sussistenza o meno, inoltre, del ruolo di amministratore di sistema (rete, infrastruttura, software o data base), dovranno ricorrere le circostanze previste dal provvedimento generale del Garante per la protezione dei dati personali "**Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008**" e successive modifiche ed integrazioni. Per quanto attiene alla figura dell'amministratore di sistema, ruoli e compiti, si rimanda alle specifiche linee guida.

Sul piano **oggettivo**, indicando la tipologia di servizio da erogare e le specifiche tecniche che caratterizzano la prestazione, identificando nel contempo eventuali condizioni vincolanti (ad es., preesistente infrastruttura su cui innestare determinati tipi di software, ovvero caratteristiche della rete che vincolano nella scelta dei software etc.).

I risultati delle suddette valutazioni confluiranno nel capitolato di gara, ovvero nella documentazione pre-contrattuale nel caso delle altre tipologie di affidamento previste dal Codice degli Appalti o infine nei contratti di fornitura o in specifici Data Protection Agreement.

4 La Titolarità del trattamento

La titolarità del trattamento, per quanto concerne le presenti linee guida, spetta comunque all'Ente (Regione toscana, Consiglio regionale, enti dipendenti), quale soggetto deputato a stabilire finalità e mezzi del trattamento di dati personali.
Pur tuttavia, nell'ambito delle forniture IT, è possibile che la determinazione dei mezzi del trattamento non sia di agevole definizione. La definizione dei mezzi del trattamento potrebbe, in effetti; essere demandata a soluzioni tecniche elaborate direttamente dal fornitore, oppure potrebbe essere richiesto al fornitore di elaborare soluzioni tecniche entro specifici limiti di importo a base d'asta. Tale circostanza, tuttavia, secondo posizione ormai consolidata del WP art. 29 (attuale Gruppo dei Garanti Data Protection europei), deve ritenersi non incidente sul ruolo di titolare del trattamento in capo all'ente. E' ammesso che un responsabile possa limitarsi a seguire orientamenti generali dati dal titolare principalmente sulle finalità senza intervenire nei dettagli per quanto riguarda gli strumenti.
Ai sensi del WP 169, *"per quanto riguarda la determinazione degli strumenti, va detto innanzitutto che il termine "strumenti" comprende evidentemente vari tipi di elementi (…). In altri termini, "strumenti" non si riferisce solo ai mezzi tecnici per trattare i dati personali, ma anche al "come" del trattamento, cioè "quali dati saranno trattati", "quali terzi avranno accesso ai dati", "quando tali dati saranno eliminati", ecc. La determinazione degli "strumenti" ingloba quindi questioni sia tecniche sia organizzative la cui decisione può anche essere delegata ai responsabili del trattamento (…). In tale ottica, è del tutto possibile che i mezzi tecnici ed organizzativi siano determinati esclusivamente dal responsabile del trattamento." In quest'ultimo caso deve essere chiarito nel contratto di servizio il ruolo del Responsabile nel determinare le misure e la loro adeguatezza e a garantire il perdurare nel tempo di tale condizione.*

5 La contrattualizzazione dei doveri del Responsabile del trattamento

Gli audit sui fornitori sono un gravame spettante al titolare del trattamento (si veda l'art. 28 comma 1, *"lett. H: messa a disposizione del titolare del trattamento "tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28", nonché consentire e contribuire "alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato"*).
Dunque, gli audit dovranno vertere su ciascun aspetto previsto dall'agreement (accordo) stipulato ai sensi dell'art. 28, in particolare:

1. rispetto di ogni istruzione del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento;
2. garanzia che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
3. adozione di tutte le misure richieste ai sensi dell'articolo 32;

4. rispetto delle condizioni generali o speciali di sub-affidamento dei trattamenti;
5. assistenza al titolare del trattamento con l'adozione delle misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III GDPR;
6. assistenza al titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
7. assistenza su rispetto degli obblighi del responsabile in relazione a cancellazione o restituzione dei dati affidati.

Peculiare attenzione deve essere rivolta ai controlli sulle misure di sicurezza, sia tecniche che organizzative, perché:

1. Aleatorie, in quanto dipendenti da fattori non solo endogeni, ma anche esogeni, come ad es. il livello accertato di cyberisk;
2. Dinamiche, dal momento che il livello di rischio muta periodicamente, ad es. con l'evoluzione tecnologica e delle tecniche di hacking.

Pertanto, le misure stabilite per effettuare i trattamenti affidati al fornitore dovranno essere oggetto di rivalutazione periodica, disciplinata dall'art. 32 GDPR secondo regole vincolanti sia per il titolare sia per il responsabile.
Tali misure coinvolgeranno e vincoleranno anche i sub-responsabili eventualmente individuati, sui quali verteranno distinti audit ad opera del responsabile.

Nota bene: *Le misure di sicurezza possono imporre gravami economici non indifferenti; per tale ragione è necessario regolamentare preliminarmente gli eventuali limiti di budget (o, in teoria, le clausole di invarianza) per la gestione delle eventuali ulteriori misure di sicurezza necessarie per rispettare i parametri di "idoneità" delle misure rispetto ai trattamenti affidati.*

6 Quando svolgere gli audit

Nel contesto degli appalti pubblici, si rinvengono due momenti fondamentali in cui è opportuno effettuare controlli sulla sussistenza delle misure a garanzia dei trattamenti affidati in outsourcing:

1. Il primo è rinvenibile in un momento immediatamente successivo all'aggiudicazione, fase in cui è necessario verificare la veridicità delle dichiarazioni rese – tra cui quelle relative alle misure di garanzia determinate a tutela dei dati il cui trattamento è appaltato. L'insussistenza delle misure determinate configurerebbe non solo mendace dichiarazione in ordine alle caratteristiche del servizio reso alla stazione appaltante, ma anche carente garanzia dei trattamenti, del che si deduce la possibilità di revoca dell'aggiudicazione dell'appalto;
2. Il secondo ricorre ciclicamente, la periodicità è determinata dal titolare sulla base del valore dei dati trattati, – deve essere perlomeno annuale e non superiore - in base alle strategie di controllo globale fissate sui propri fornitori.

7 Modalità di svolgimento degli audit

In relazione ai controlli ciclici, alcuni indici utili a determinare le priorità del piano di audit sono:

1. Forniture critiche; la criticità delle forniture si rinviene da indici non tassativamente previsti, inerenti a fattori che possono riguardare o direttamente il trattamento dei dati personali, come il livello di rischio del trattamento affidato in appalto o fattori esterni come l'importo dell'appalto.
2. Forniture per le quali, in precedenti audit, sono state segnalate azioni di remediation per l'adeguamento delle misure di sicurezza (follow up)
3. Forniture selezionate a campione (a seguito della verifica delle precedenti forniture prioritarie)
4. Le modalità di audit, secondo le best practices consolidate, possono essere ricondotte a scenari:
    1. Ricognizione generale delle misure adottate, anche tramite autodichiarazione resa dal fornitore;
    2. Verifica delle dichiarazioni rese ai sensi del precedente punto;
    3. Verifica in loco delle misure adottate.

8 L'audit report e il remediation plan

Al termine dell'audit il Titolare del trattamento, attraverso le sue strutture tecniche di riferimento, fornirà al Responsabile, un audit report, contenente le carenze riscontrate in materia di protezione dei dati personali, in relazione agli aspetti controllati ed elencati nei precedenti paragrafi.
In base alle risultanze dell'audit report, sarà opportuna, a cura del Responsabile, l'elaborazione di un "piano di remediation" finalizzato a colmare le carenze evidenziate. Lo stesso sarà condiviso con il Titolare, che effettuerà il follow up conseguente, per verificare la corretta implementazione degli aspetti risultati non ottimali.
Il piano di remediation dovrà contenere il dettaglio delle attività di adeguamento che il fornitore si impegna ad integrare e le relative scadenze, concordate con il Titolare. Su tale contenuto il Titolare del trattamento, come già sopra specificato, effettuerà successivi controlli per verificare il compimento delle azioni correttive.
Risulta utile sottolineare che il Titolare, nello svolgimento di questi compiti si avvarrà delle strutture tecniche interne dell'ente ed in particolare del responsabile del contratto, del direttore esecutivo del contratto e se necessario del security IT manager.

9 Riepilogo dei controlli

In sintesi possiamo asserire che i controlli da porre in essere, sono sia formali, sia di merito.
I controlli possono e debbono essere messi in atto, sia in un momento successivo alla stipula del contratto, data che deve essere dichiarata nel capitolato (nel contratto deve essere esplicitata la sua risoluzione in caso di verifica negativa), sia periodicamente secondo un piano temporale anch'esso indicato nel contratto, sia ogni qual volta si verifichi un incidente.
E' opportuno che ogni ente, nel suo ruolo di Titolare, definisca con il supporto del Security IT Manager, un piano pluriennale dei controlli (Audit), che tenga conto delle criticità o meno dei servizi utilizzando come criterio guida la valutazione di rischio in relazione alla tipologia dei dati trattati, alle categorie degli interessati coinvolti, della numerosità degli stessi (elementi che determinano il "valore del dato" trattato).
I controlli possono sempre essere assistiti dal DPO o dalla sua struttura. Per alcuni controlli di merito occorre coinvolgere il Security IT Manager o persone da lui indicate con adeguata professionalità.
Gli esiti dei controlli debbono essere comunicati al DPO, al RUP e al DEC del contratto di fornitura ognuno per gli aspetti di propria competenza.

9.1 Controlli formali

I controlli formali debbono riguardare l'esistenza della documentazione richiesta per rispondere al principio della accountability e per consentire al Titolare di conoscere e saper documentare la corretta relazione con il Responsabile, anche nelle ispezioni del Garante o di auditing interni all'ente.

9.1.1. Data Protection Agreement

Il documento di Data Protection Agreement deve essere sottoscritto fra le parti prima della erogazione del servizio e deve essere aggiornato ogni qual volta cambino i trattamenti o le relative misure di sicurezza.

9.1.2. Registro dei trattamenti

Il registro dei trattamenti deve essere attivato e i trattamenti registrati e firmati prima della messa in esercizio del servizio. Il registro deve essere completo, deve cioè contenere tutti i trattamenti messi in atto, e per ogni trattamento devono essere compilate tutte le informazioni relative alla liceità, alla descrizione del trattamento, alla individuazione del titolare e del responsabile/sub responsabile, agli asset, alle misure di sicurezza, agli autorizzati, ecc.. Il registro deve essere firmato, deve consentire una ricostruzione storica delle registrazioni, deve essere facilmente accessibile e consultabile in fase di ispezione da parte del Titolare o del Garante.

9.1.3. Autorizzati

Deve essere immediatamente disponibile, su richiesta e tramite estrazione dal registro dei trattamenti, l'elenco degli autorizzati e dei relativi profili per ogni trattamento. Il formato dei dati deve essere elaborabile con strumenti digitali.

9.1.4. Amministratori di sistema

Deve essere disponibile l'elenco degli amministratori di sistema con indicazione degli asset di riferimento. (Data Base amministrator, System Amministrator, ecc..). L'elenco deve essere immediatamente disponibile su richiesta e deve essere consegnato con un formato elaborabile con strumenti digitali.

9.1.5. Informazioni agli operatori/autorizzati

Occorre verificare che tutti gli operatori (amministratori di sistema, autorizzati, altro personale), che possono venire a vario titolo in contatto con i dati personali, abbiano ricevuto adeguata informazione, che siano impegnati alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

9.1.6. Gestione degli asset

Verificare l'esistenza del catalogo degli asset con i seguenti contenuti:

a) Descrizione complessiva dell'architettura tecnologica (servizi Infrastrutturali), IaaS, PaaS, SaaS del Responsabile nella quale si evidenzino le eventuali diverse zone (ambiti architetturali), a diversa intensità di sicurezza (bassa, media, alta);
b) Descrizione dei servizi Applicativi o in Modalità SaaS;
c) Descrizione dei servizi applicativi eventualmente gestiti da altri fornitori ma ospitati nell'infrastruttura del Responsabile o viceversa;
d) Collegamento con le misure di sicurezza;
e) Collegamento con i trattamenti;
f) Descrizione dei processi organizzativi che sovraintendono la gestione degli asset ed il loro continuo aggiornamento per quanto attiene anche alle misure di sicurezza.

9.1.7. Misure di sicurezza

Occorre verificare che esista la documentazione che descriva per ogni asset le misure di sicurezza adottate, valutate e dichiarate adeguate in relazione alla tipologia di dati personali trattati (livello di rischio definito sulla base della tipologia di dati, categorie di interessati, numerosità degli interessati). Questo richiede che il Responsabile tenga strettamente correlati, attraverso il registro, i trattamenti con gli asset e quindi con le misure di sicurezza.
Particolare attenzione deve essere posta alle misure di sicurezza adottate per il processo di identificazione e attribuzione dei ruoli e dei profili agli autorizzati come alle altre categorie di misure di sicurezza elencate nel documento "Misure di sicurezza e loro classificazione".
Le misure di sicurezza debbono sempre riferirsi per la loro adeguatezza ai dati contenuti e trattati, pertanto occorre considerare le misure di sicurezza complessivamente applicate ai dati, partendo da quelle applicative fino a quelle logistiche.

9.1.8. Gestione degli incidenti

Occorre verificare che il Responsabile abbia messo in esercizio il "registro degli incidenti" e definito una procedura organizzativa interna idonea ad intercettare gli incidenti e gestire efficacemente il processo di rilevamento, di comunicazione al titolare e di conduzione della gestione dell'incidente stesso ivi compresa la formulazione e la messa in atto di un remediation plan.

9.1.9. Piano di qualità della fornitura

Deve esistere un piano di qualità della fornitura nel quale occorre che insieme ad altre cose che possono riguardare la fornitura dei servizi, siano descritti:

- L'organizzazione del responsabile con riferimento alle figure di presidio dei processi GDPR;
- Relazioni con sub responsabili o con altri soggetti nella gestione della conduzione dei servizi che prevedono il trattamento di dati personali e dei processi GDPR;
- Processi messi in atto per il rispetto del GDPR (rispetto della DPA, Accountability, Data Protection by Default by Design, Diritti degli interessati, Gestione degli incidenti);
- Processo di deployment dei servizi applicativi e non;
- Registro delle applicazioni e dei profili di accesso e autorizzazione (quali azioni e su quali dati);
- Processo di audit interno per la verifica delle misure di sicurezza;
- Modalità di gestione congiunta con altri soggetti con particolare riferimento a:
    a. Processi produttivi,
    b. Gestione degli asset,
    c. Gestione del registro dei trattamenti,
    d. Gestione del registro, degli incidenti e relativi processi di detection, notifica, problem determination, remediation plan,
    e. Gestione complessiva delle misure di sicurezza e dichiarazione della loro adeguatezza
    f. Gestione congiunta degli audit interni.

9.1.10. Check list controlli formali

A titolo esemplificativo :

Controlli Formali	***Esistenza*** *(Si/No)*	***Livello completezza/aggiornamento*** *(Basso, Medio, Alto)*	***Note*** *(Carenze da superare)*
Data Protection			

Agreement			
Registro dei Trattamenti			
Elenco Autorizzati			
Elenco amministratori di sistema			
Informazione agli operatori			
Gestione degli asset			
Misure di sicurezza			
Gestione degli incidenti			
Piano di qualità della fornitura			

9.2. Controlli di merito

I controlli di merito sono finalizzati a verificare la corrispondenza fra quanto dichiarato e aunto messo in atto oltre a rilevare punti di debolezza del sistema. Per questa attività occorre che il Titolare ricorra a specifiche e verificate professionalità.

9.2.1. Data Protection Agreement

Occorre verificare che quanto descritto nel DPA sia conforme ed aggiornato a quanto risulta dal registro dei trattamenti, e in eventuali sub forniture che siano nel frattempo intervenute o modificate.

9.2.2. Registro dei trattamenti

Occorre verificare in relazione alle applicazioni effettivamente in esercizio, tramite la rilevazione sul campo (es. elenco dei servizi indirizzati dagli application server), se esse siano presenti nel catalogo degli asset e questi siano collegati ai relativi trattamenti e alle relative misure di sicurezza (attraverso il registro dei trattamenti). Occorre verificare la coerenza dei nomi fra gli asset applicativi nel registro dei trattamenti e quanto effettivamente gestito.

9.2.3. Autorizzati

I Responsabile deve, a richiesta, rendere immediatamente disponibili:

a) i log degli accessi degli utenti alle applicazioni sotto audit,
b) gli autorizzati presenti nel registro dei trattamenti con riferimento alle applicazioni (asset);

ambedue gli elenchi in formato elaborabile digitalmente in modo da poter essere confrontati.
Per ogni autorizzato deve essere possibile ottenerne il profilo autorizzativo di accesso all'applicazione (autorizzazione) ma anche e soprattutto di accesso alle funzioni interne dell'applicazione (profilo applicativo) attraverso il quale sia possibile risalire in modo semplice alle azioni che l'autorizzato può fare sui dati e su quali dati. I file di log devono consentire di verificare quali siano state le funzioni utilizzate dall'autorizzato o da un utente.
Il controllo dovrà verificare che tutti gli utenti presenti sui log siano anche presenti nella lista degli autorizzati e che il profilo di accesso sia compatibile con la descrizione del trattamento a cui sono autorizzati.

9.2.4. Amministratori di sistema

Occorre controllare che le credenziali di accesso siano univocamente assegnate ad una ed una sola persona e che esistano dei file di log che possano indicare per ogni persona l'accesso indicando i parametri temporali e i contenuti.
Occorre ottenere:

a) I file di log dei sistemi con l'indicazione della persona,
b) L'elenco degli amministratori di sistema.

Sulla base di questi elenchi occorre poter verificare che tutte le persone che hanno operato come amministratori di sistema siano presenti nell'elenco che non esistano conflitti di interesse (separation of duty), che le credenziali di accesso siano rinnovate con un periodo consono alla delicatezza dei dati trattati.

9.2.5. Informazioni agli operatori/autorizzati

Occorre verificare, tramite interviste, se gli operatori hanno effettivamente recepito le indicazioni di riservatezza delle quali sono stati informati e quali comportamenti hanno adottato in conseguenza delle informazioni ricevute.

9.2.6. Misure di sicurezza

Per la verifica nel merito delle misure di sicurezza, si rimanda al documento "misure di sicurezza e loro classificazione" e non possono che essere demandate, dal titolare, a personale specializzato.
Tale controllo è finalizzato ai seguenti scopi:

a) Verificare se le misure dichiarate siano effettivamente messe in campo;
b) Verificare che i processi di aggiornamento delle misure di sicurezza siano attivi;
c) Verificare l'adeguatezza delle misure di sicurezza in relazione al livello di rischio dei dati trattati.

9.2.7. Gestione degli incidenti

Occorre prendere visione del registro e farne:

a) Una valutazione complessiva di rispondenza alla realtà;
b) Una verifica di completezza delle informazioni riportate;
c) Una verifica se i remediation plan siano poi stati attuati.

9.2.8. Piano di qualità della fornitura

Occorre verificare se quanto dichiarato nel piano di qualità della fornitura risponde, nell'organizzazione e nei processi, a quanto rilevabile sul campo.

9.2.9. Check list controlli di merito

A titolo esemplificativo:

Controlli di Merito	*(Si/No)*	***Livello*** *(Basso, Medio)*	***Note*** *(Carenze da superare)*
Data Protection Agreement: 1. Congruenza con registro trattamenti 2. Congruenza con misure di sicurezza			
Registro dei Trattamenti 1. Congruenza dei trattamenti con le applicazioni in esercizio 2. Congruenza delle applicazioni con gli asset registrati			
Elenco Autorizzati			

1. Congruenza degli autorizzati dichiarati con quelli effettivi nei log			
Elenco amministratori di sistema 1. Congruenza degli amministratori di sistema dichiarati con quelli effettivi nei log.			
Informazione agli operatori 1. Verifica, tramite interviste, che gli operatori siano stati effettivamente informati			
Gestione degli asset 1. Verifica che gli asset rilevati siano presenti nel catalogo con adeguato livello di descrizione			
Misure di sicurezza 1. Verifica se le misure dichiarate siano effettivamente messe in campo, 2. Verifica che i processi di aggiornamento delle misure di sicurezza siano attivi, 3. Verifica della adeguatezza delle misure di sicurezza in relazione al livello di rischio dei dati trattati.			
Gestione degli incidenti 1. Una valutazione complessiva di rispondenza alla realtà, 2. Una verifica di completezza delle informazioni riportate 3. Una verifica se i remediation plan siano poi stati attuati			
Piano di qualità della fornitura 1. Verifica dell'attuazione organizzativa 2. Verifica dell'attuazione dei processi			

Accordo fra Fornitori

Schema DPA P2P

1 Scopo

Il presente documento ha l'obiettivo di definire uno schema di contratto GDPR (DPA) fra fornitori (Responsabili) che contribuiscono, attraverso contratti di fornitura diversi, allo sviluppo e gestione di un unico sistema informativo che prevede il trattamento di dati personali, e a motivarne l'esigenza a tutela del Titolare.

2 Premessa

Al fine di meglio comprendere la problematica oggetto del presente documento si propone un esempio concreto della Regione Toscana.

La Regione Toscana, attraverso una procedura di gara nella sua funzione di soggetto aggregatore, ha rivisitato e aggiudicato ad un nuovo soggetto la gestione del Sistema Cloud Toscana (ex TIX).
SCT offre servizi, nella stragrande maggioranza di tipo IaaS (risorse di rete, risorse computazionali risorse di memorizzazione) e PaaS (ambienti quali sistemi operativi, basi di dati, ecc..) e solo in alcuni casi (vedasi la Posta elettronica) del tipo SaaS. I servizi di tipo IaaS e Paas non realizzano direttamente servizi di trattamento dati ma forniscono risorse tecnologiche alle applicazioni che costituiscono la vera componente predisposta al trattamento di dati, fra cui quelli personali. Pertanto l'erogazione di un servizio che prevede il trattamento di dati, viene ad essere realizzato attraverso una applicazione (un software) che definisce, attraverso la sua logica elaborativa, come e quali dati vengono trattati e da chi. Lo sviluppo e gestione delle applicazioni, nonché i servizi collaterali come l'Help desk di secondo livello, sono garantiti da un fornitore di norma diverso da quello con il quale si sono contrattualizzati i servizi SCT. Pertanto la erogazione di un servizio (trattamento) all'utente finale, coinvolge sia il soggetto gestore di SCT, sia il fornitore della componente applicativa.

Forniture, queste, che sono contrattualizzate, attraverso contratti diversi, con diversi fornitori.

Occorre ricordare come quello a cui tendere e garantire, sia un sistema sicuro e chela sicurezza complessiva è costituita dall'insieme coordinato e coerente delle misure di sicurezza, riferite alle singole componenti. Sicurezza a livello di rete, sicurezza a livello di basi di dati, sicurezza delle componenti operative, sicurezza nell'accesso, sicurezza dei dati, ecc..
Risulta ovvio quindi, come sia indispensabile, al fine di garantire le adeguate misure di sicurezza a tutela dei diritti degli interessati, così come richiesto dal GDPR, un accordo fra il soggetto gestore di SCT e il fornitore/i della componente applicativa. Occorre che i due soggetti siano solidali nel garantire la sicurezza dei sistemi e dei servizi, ben sapendo che la sicurezza complessiva non si realizzata come somma algebrica delle singole misure di sicurezza e che la sicurezza della catena è rappresentata dal suo anello più debole.
Occorre un accordo, certo non facile da realizzare ma non per questo da non perseguire, fra i due fornitori nel quale si definiscono i compiti di ciascuno, singolarmente o in team, al fine di garantire al titolare una impostazione e una gestione del servizio nel suo complesso sicura in modo proporzionato al "valore dei dati trattati".

Tale accordo costituisce di fatto una tipologia di DPA, che chiameremo Processor to Processor (P2P), che regola i rapporti fra differenti Processor (responsabili) quando concorrono agli obiettivi e procedure del Titolare attraverso contratti diversi. Infatti se esistesse un unico contratto che lega tutti i soggetti coinvolti nella erogazione del servizio, saremmo nella tipologia di DPA Titolare Responsabile.

Sta nelle prerogative e obblighi del Titolare controllare e garantire la sicurezza per tutti i trattamenti di propria competenza, regolando e dando specifiche istruzioni, a coloro ai quali assegna il compito della erogazione dei servizi, per la tutela dei diritti degli interessati.
Pertanto qualora un servizio, inteso come un insieme di trattamenti di dati personali, viene assicurato da fornitori diversi con differenti contratti, il titolare deve regolare i rapporti fra i diversi fornitori, in modo da garantire, attraverso misure tecniche ed organizzative, la tutela dei diritti e delle libertà degli interessati.
Lo schema di DPA suggerito in questo documento ha lo scopo di regolare i rapporti fra i diversi fornitori al fine di definire ruoli e responsabilità di ciascuno.
Tale problematica riguarda la Regione Toscana ma anche tutti gli enti che decidessero di portare le loro applicazioni all'interno delle infrastrutture di SCT.
E riguarda sempre e comunque le situazioni in cui alla erogazione di un servizio concorrono più soggetti attraverso contratti diversi.

Qualora non fossero stati formalizzati i DPA verso i singoli fornitori, il DPA P2P li sostituisce, altrimenti li integra.

3 Schema DPA P2P

Nel DPA sottoscritto dai due o più fornitori e dal titolare devono essere presenti i successivi capitoli:

3.1. Oggetto dell'accordo

In questo capitolo si riportano:

1) Gli estremi identificativi dei due Processor;
2) I riferimenti ai contratti di fornitura di servizi;
3) I riferimenti ai rispettivi DPA se esistenti;
4) La descrizione sommaria dei servizi erogati agli interessati;
5) Le implicazioni rispetto al GDPR e relative figure.

3.2. Valutazione della rilevanza dei dati trattati

In questo capitolo si riportano:

1) La tipologia di dati personali trattati;
2) Le categorie degli interessati;
3) La Numerosità degli interessati coinvolti
4) La tipologia delle misure adottate in conseguenza con riferimento al documento **Valutazione *Misure di Sicurezza,*** per la valutazione del *"valore dei dati"* trattati e il livello di misure di sicurezza da adottare.

[Sulla base di questi dati si valuta, congiuntamente fra Titolare e fornitori, la rilevanza dei dati trattati al fine di assicurare le adeguate misure di sicurezza valutando i rischi, le minacce, le contromisure e andando a determinare il rischio residuo ritenuto accettabile dal Titolare.]

3.3. Descrizione del sistema

*[In questa sezione si descrive il sistema nel suo complesso in **termini di servizi** per l'utente, e di quelli messi in atto per tutelare e rispondere ai diritti degli interessati]*

3.3.1. Servizi per gli utenti finali

[In questa sezione si descrivo i servizi]

3.3.1.1. Livelli relativi alle misure di sicurezza

*[In questa sezione per ogni servizio garantito si andranno a descrivere i livelli di sicurezza assicurati in relazione ai diversi rischi e al **valore dei dati** trattati]*

3.3.1.2 Livelli relativi alla diponibilità del servizio

[In questa sezione per ciascun servizio garantito si andranno a descrivere i livelli di disponibilità dei servizi stessi andando a descrivere le misure adottate]

3.4. Impegni e ruoli ai fini della protezione dei dati

[In questa sezione si riprende, rivisto, quanto descritto nella DPA Titolare-Responsabile e si regolano a norma del GDPR le relative figure]
In particolare si vanno a descrivere come avviene la gestione congiunta o correlata:

1. *del registro dei trattamenti,*
2. *della gestione del catalogo degli asset,*
3. *degli elenchi degli autorizzati*
4. *degli amministratori di sistema*
5. *delle misure di sicurezza*
6. *della gestione degli incidenti*

al fine di garantire al Titolare semplicità nel rispondere a quanto richiesto dal processo di Accountability sia nei confronti del Garante sia degli interessati.

3.5. Descrizione delle componenti del sistema complessivo

[In questa sezione si andranno a descrivere le diverse componenti di sistema intese come la catena degli asset che sostengono la erogazione del servizio e dell'insieme di servizi, partendo dall'applicativo/servizio verso gli utenti finali.]

3.5.1. Responsabile 1 (fornitore)

3.5.1.1. Componenti del sistema in carico

[Facendo riferimento al capitolo precedente si indicano le componenti che sono in carico al Responsabile 1.]

3.5.1.2 Misure di sicurezza adottate

[Con riferimento alle componenti di cui al punto precedente si descrivono in relazione ai principali rischi le misure adottate al fine della loro mitigazione]

3.5.2. Responsabile 2 (fornitore)

3.5.2.1. Componenti del sistema in carico

[Facendo riferimento al capitolo precedente si indicano le componenti che sono in carico al Responsabile 2.]

3.5.2.2. Misure di sicurezza adottate

[Con riferimento alle componenti di cui al punto precedente si descrivono in relazione ai principali rischi le misure adottate al fine della loro mitigazione]

3.6. Organizzazione per la sicurezza

[In questo capitolo si descrive l'organizzazione congiunta dei due responsabili e le procedure idonee a garantire il continuo aggiornamento delle misure di sicurezza.]

3.6.1. Deployment delle applicazioni

(modalità e livelli di servizio per tutto il ciclo di vita delle applicazioni)

3.6.2. Team della sicurezza

(costituzione (può prevedere o meno una persona del Titolare con adeguate competenze tecniche) , obiettivi, procedure, comunicazioni)
Il responsabile del *Team Sicurezza* acquisisce il ruolo di referente unico nei confronti del Titolare nel processo di gestione degli incidenti, nell'attuazione del remediation plan, nella formazione delle DPIA, nei processi di Audit del Titolare/DPO, nel supporto al titolare in fase di ispezione del Garante, nel proporre interventi migliorativi nelle misure di sicurezza al cambiare della tecnologia, al modificarsi delle minacce, alla conoscenza di bugs sui sistemi o sul middleware, alla obsolescenza di versioni o release di software, ecc.. Dovrà essere compito del responsabile del team della sicurezza redigere periodicamente un assessment complessivo sulle misure di sicurezza e sulla loro adeguatezza o meno indicando, in quest'ultimo caso, gli interventi da fare e la loro tempistica. Tale relazione deve essere inviata al Titolare e al DPO e ad altri sulla base del modello organizzativo adottato.

Nota: Il responsabile del Team può essere una persona del Responsabile 1 o del Responsabile 2 o anche della struttura organizzativa del Titolare.

3.6.2.1. Gestione degli incidenti

[Descrivere il processo di gestione degli incidenti, della loro detection, della notifica, del problem determination e relativo remediation plan, con indicazione dei rispettivi ruoli e compiti.]

3.6.2.2. Audit Interno e impegni congiunti

[descrizione delle Modalità di esecuzione, dei tempi, delle azioni susseguenti le risultanze]

3.6.2.3. Servizi per la tutela degli interessati (capo III) GDPR

[In questo capitolo si descrivono i servizi che congiuntamente i Responsabili debbono garantire al Titolare al fine di garantire i diritti degli interessati]

3.7 Dichiarazione congiunta sulla adeguatezza a norma GDPR delle misure adottate

Al momento della stipula del presente accordo viene effettuata una valutazione complessiva sull'adeguatezza delle misure di sicurezza adottate che sarà successivamente aggiornata periodicamente, secondo quanto previsto dai processi di audit e di gestione degli incidenti.
[In questo capitolo, allegando la eventuale DPIA, formale o comunque utilizzando il modello di correlazione Rischi, Minacce, contromisure si descrive il ragionamento e le valutazioni in merito alla adeguatezza delle misure tecniche e dei processi di gestione, al "valore dei dati" trattati.]
Si evidenziano processi e procedure da mettere in atto al fine di garantire il non decadimento delle misure adottate e valutate]

F.to Responsabile 1 _____
F.To Responsabile 2 _____
F.to Titolare: _____

Misure di sicurezza e loro classificazione
Linee guida

1 Scopo

Il presente documento ha lo scopo di fornire le linee guida, una metodologia, per determinare il "valore del dato" trattato e correlarlo ai livelli delle misure di sicurezza ed avere indicazioni circa l'adeguatezza delle stesse. Tali considerazioni sono inoltre utili al fine della formulazione delle DPIA.

2 Premessa

Gli standard internazionali, siano essi gli ISO europei o Il NIST americano, in relazione alle misure di sicurezza dei sistemi IT, individuano controlli di sicurezza e relativi livelli prendendo in esame le esigenze di integrità, riservatezza, affidabilità e continuità operativa. Sono individuati tre livelli, basso, medio ed alto sulla base di considerazioni generali di sicurezza.
L'introduzione del GDPR richiede di porre ulteriore attenzione al "valore del dato" personale determinato sulla valutazione dei rischi per i diritti e libertà dell'individuo a cui quelle informazioni si riferiscono.
Il GDPR richiede pertanto di aggiungere, alle considerazioni presenti nella valutazione delle misure da adottare sui sistemi IT, il ***valore del dato*** trattato.

3 Valore del dato

Dall'articolo 4 del GDPR si evince che un dato personale è una qualsiasi informazione che permette di identificare in maniera univoca un singolo individuo attraverso le sue caratteristiche, le sue relazioni personali, le sue abitudini, il suo stile di vita e così via, Personal Identifiable Information (PII). Tali informazioni vengono classificate a seconda della loro tipologia in comuni, particolari e giudiziarie.
Inoltre nella determinazione del rischio per le libertà e i diritti degli interessati, rientra anche la categoria degli interessati a cui le informazioni si riferiscono, in quanto riferendosi a categorie più o meno deboli di persone e che pertanto possono ricevere un danno variabile in rapporto al loro stato.
Infine la numerosità delle persone per le quali le informazioni personali vengono trattate rappresenta un ulteriore parametro da tenere presente nella determinazione del rischio.
Sarà quindi sulla base di questi tre parametri, tipologia del dato, categorie degli interessati e numerosità degli stessi, che si andrà a determinare il "valore del dato" e le relative misure di sicurezza da applicare ad esso.

3.1. TIPOLOGIA DI DATO PERSONALE

Rientrano pertanto in questa categoria tutte le informazioni cosiddette "comuni", informazioni cosiddette particolari (ex dati sensibili) e quindi da sottoposte a tutela particolare, e le informazioni giudiziarie che possono rilevare l'esistenza di provvedimenti giudiziari a carico dell'individuo.
L'utilizzo di nuove tecnologie infine ha esteso il concetto di dato personale anche ai dati relativi alle comunicazioni elettroniche via telefono o internet (indirizzo IP, cookie ID, ecc.), ai dati che consento la geolocalizzazione della persona, ai dati genetici o biometrici.
I dati particolari (definiti anche "particolarmente sensibili" all'interno del considerando nr. 10 e nr. 51) sono dati personali che sono oggetto di una maggior tutela in quanto possono rilevare aspetti connessi alla sfera più intima dell'individuo. Tali dati sono quelli a cui fa riferimento l'art. 9 del GDPR:
"*E' vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati*

biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".
Sono da considerarsi dati giudiziari tutti i dati relativi a condanne penali e a reati ovvero dati che possono rilevare l'esistenza di determinati provvedimenti giudiziari soggetti a iscrizione nel casellario giudiziale (es: provvedimenti penali di condanna definitivi, divieto e obbligo di soggiorno, misure alternative al carcere, ecc.) o rivelare la qualità di imputato o di indagato.

3.2. CATEGORIE INTERESSATI

L'interessato al trattamento è la persona fisica a cui si riferiscono i dati personali e che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Le linee guida in materia di valutazione di impatto sulla protezione dei dati (WP248) pubblicate dal gruppo di lavoro dei garanti europei individua nei dati relativi a interessati vulnerabili uno dei 9 criteri da considerare per valutare se una particolare tipologia di trattamento richieda una valutazione d'impatto sulla protezione dei dati o meno.
Gli interessati vulnerabili possono includere i minori (i quali possono non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento. Questo squilibrio di potere fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Dato che la normativa europea per la protezione dei dati prevede una tutela rafforzata per la categoria dei minori.

3.3. NUMERO DI PERSONE COINVOLTE NEL TRATTAMENTO

Il numero di persone coinvolte nel trattamento rappresenta uno dei fattori da tenere in considerazione al fine di stabilire il "livello di scala" di un trattamento.
Il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. In linea di massima si intende per trattamenti su larga scala la gestione di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato.

4 Misure di sicurezza aggiuntive per i trattamenti di dati personali

Questo documento individua inoltre i ***livelli delle misure di sicurezza aggiuntive*** (LMSA) per il trattamento di dati personali (PII). Questi livelli di sicurezza aggiuntivi vanno a soprapporsi integrandoli ai controlli di sicurezza predeterminati senza la valutazione del dato trattato secondo i principi del GDPR. I LMSA identificano specifici "valori nei controlli di sicurezza" richiesti per proteggere le informazioni di identificazione personale (PII), nell'ambito di sistemi IT e sono volti a ridurre i rischi per gli interessati durante l'intero ciclo di vita delle informazioni. I LMSA supportano l'implementazione, ma non intendono e non sostituiscono i requisiti di Data Protection previsti dalla normativa o nei regolamenti.
Tali indicazioni, come detto, non sostituiscono, ma si aggiungono alle misure di sicurezza tese a garantire l'integrità, la riservatezza, la affidabilità e la continuità dei sistemi IT e dei servizi digitali, cosi come definiti in termini di standard e controlli ISO che tutte le organizzazioni dovrebbero attuare.

Nello specifico ci riferiamo a quelli adottati dalla Regione Toscana nell'ambito del proprio "Framework per la sicurezza IT" (FSIT)

Il GDPR ha stabilito alcuni principi fondamentali fra cui la Data Protection by design e by default e il ***principio di adeguatezza*** nel definire le misure di sicurezza in relazione al valore dei dati trattati.

I controlli di sicurezza, che sono gli stessi degli standard NIST o ISO, attraverso i LMSA, forniscono un approccio coerente per implementare "adeguate garanzie amministrative, tecniche e fisiche" per proteggere le PII nell'ambito dei sistemi informativi digitali. Tutte le PII, come abbiamo visto, non sono ugualmente sensibili, non hanno lo stesso *valore* e quindi non tutte le PII richiedono la stessa protezione; PII con valore più elevato richiedono protezioni più rigorose, mentre PII con valore inferiore richiedono protezioni meno rigorose.
Nella nostra impostazione sono individuate tre LSMA che correlano il valore delle PII ai valori dei controlli di sicurezza, andando ad individuare tre livelli: Basso, Moderato o Medio e Alto.

Le PII che si riferiscono a dati sanitari vengono individuati, nei documenti tecnici internazionali, con la sigla PHI e costituiscono quindi un sottoinsieme delle PII. Il trattamento delle PHI, oltre alle considerazioni relative al valore del dato, richiede ulteriori considerazioni che riguardano l'esigenza di poter ricomporre il dato anagrafico con il dato sanitario per specifici scopi di ricerca, di difesa della salute pubblica o altre motivazioni individuate tramite specifiche normative. Pertanto PHI individua un quarto livello di valorizzazione o specializzazione dei controlli.
I controlli di sicurezza e la loro valorizzazione per i diversi LMSA devono essere valutati e rivisti qualora si modifichi il quadro normativo o regolamentare, pertanto mantenerli correlati e non integrati con il valore delle PII, consente una facile attività di revisione salvaguardando l'impostazione complessiva
Per raggiungere questi obiettivi distinti, gli LMSA forniscono livelli indipendenti per supportare la conformità ai requisiti del GDPR. Gli LSMA aiutano i Titolari, i responsabili della sicurezza dei sistemi di informativi, i gestori dei sistemi, i gestori delle applicazioni, gli sviluppatori ecc., identificando le specifiche di sicurezza e controllo della Data Protection. I professionisti della sicurezza e della Data Protection hanno spesso fra loro background e livelli di comprensione diversi per le esigenze e le attività reciproche. Gli LMSA includono informazioni per aiutare le comunità di gestione della Data Protection e della sicurezza a capirsi e a collaborare per proteggere le informazioni personali. Un linguaggio comune fra chi affronta con diverse competenze il tema della protezione dei dati personali. È fondamentale che gli uffici che si occupano di IT e gli uffici che si occupano di data protection collaborino, trovino un linguaggio comune, in fase di progettazione dei sistemi e che la collaborazione continui per tutto il ciclo di vita del sistema IT.
Questa collaborazione interdisciplinare, che vede giuristi, organizzatori e tecnici IT è fondamentale al fine di garantire il principio di Data Protection by design and by default.

4.1 Correlazione fra valore del dato e livelli di misure di sicurezza

Correlare il valore del dato alle misure di sicurezza da adottare, è uno dei compiti primari nella fase di progettazione di un sistema informativo o di singoli servizi digitali, e richiede una stretta collaborazione fra chi conosce il contesto, di norma il titolare, e le strutture tecniche predisposte alla progettazione e realizzazione siano esse interne all'organizzazione del Titolare o esterne (Responsabile).

Nella fase di progettazione secondo il principio di Data Protection by Design, by Default, devono essere valutate e classificate le PII al fine di definire quale LMSA, (basso, medio, alto) o PHI, applicare.
Pertanto risulta importante e fondamentale che il prima possibile, negli atti che danno il via alla realizzazione o modifica sostanziale di un sistema informativo si produca la "Scheda Data Protection" che, descrivendo i dati personali coinvolti, costituisce un importante e rilevante input per al progettazione tecnica ed organizzativa. Si ricorda che gli elementi della "Scheda data protection", devono essere presenti in tutti i Data Protection Agreement, assieme alla descrizione delle misure di sicurezza adottate.

Si riporta, nelle tabelle seguenti e in modo sintetico, il processo per la classificazione delle PII e la loro correlazione con i livelli delle misure di sicurezza (LMSA) basso, medio, alto e PHI.
A questi livelli vengono associati "controlli generali" derivanti da valutazioni in merito alla esigenza di integrità, riservatezza, affidabilità e continuità dei sistemi così come discendono dagli standard ISO o dalle indicazioni del NIST americano, a cui si aggiungono i ***LMSA*** per il trattamento di dati personali (PII, Personally Identifiable Information). Pertanto in dipendenza del valore del dato personale si vanno ad attuare tutti i "controlli di sicurezza" tenendo presente, per ciascuno di essi, i livelli delle misure di sicurezza e i livelli delle misure di sicurezza aggiuntivi derivanti dall'analisi delle PII trattate.

In questo documento ci riferiamo solo ai livelli delle misure di sicurezza aggiuntive, lasciando alle politiche della sicurezza dell'ente quelle che si applicano secondo altre valutazioni.

Il metodo per determinare il "valore" del dato personale (PII), come detto in precedenza, si basa su tre parametri, la tipologia di dati, le categorie degli interessati, la numerosità degli stessi.
Nella Tabella 1 si riportano i parametri della tipologia di dati e delle categorie degli interessati andando ad individuare un indicatore che ci dia la misura dell'attenzione che dobbiamo porre ai trattamenti: "Ranking di attenzione".

Tabella1: Ranking di attenzione

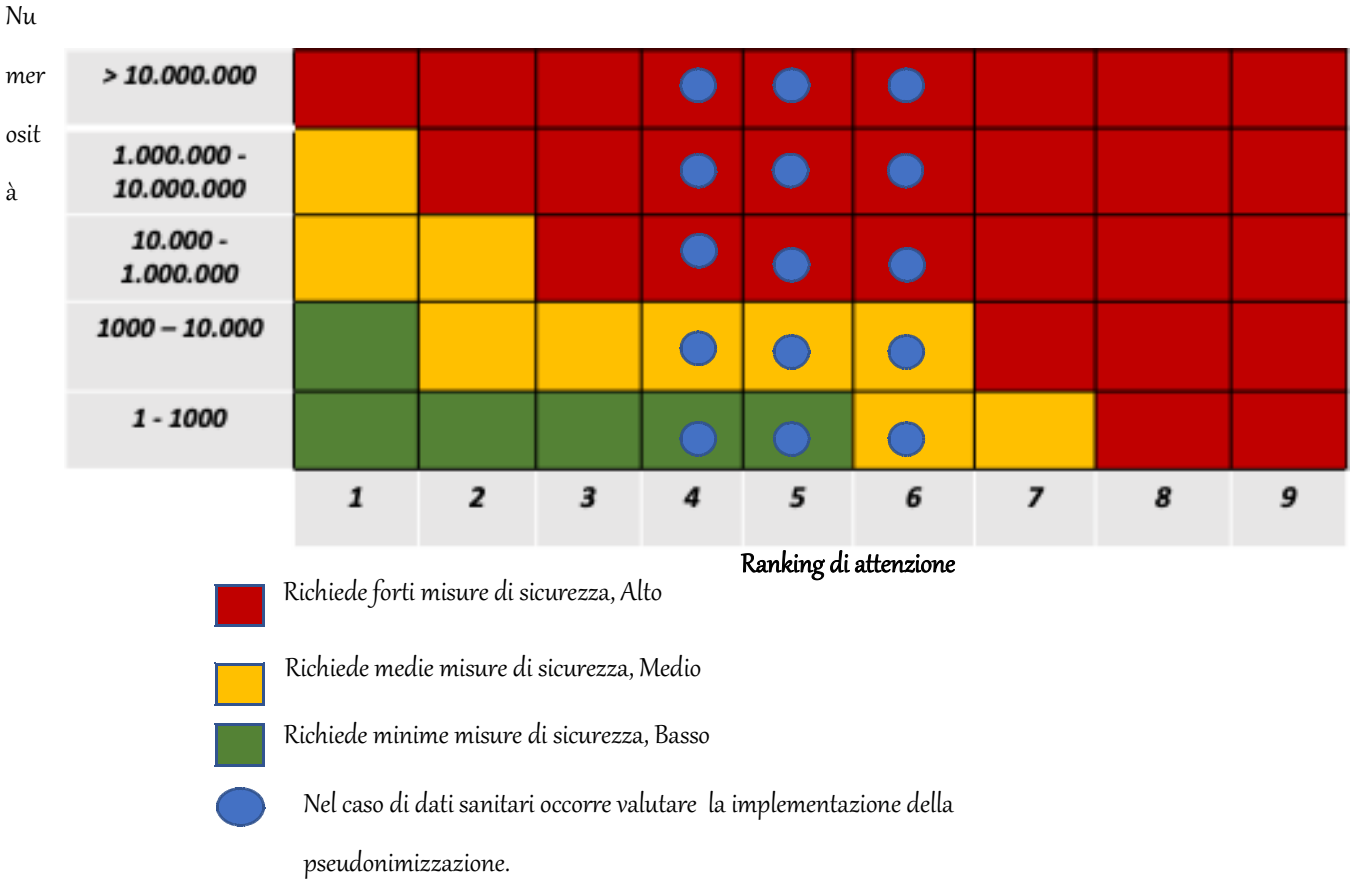
Tipologia di dati			
Giudiziari	7	8	9
Particolari	4	5	6
Comuni	1	2	3
	Comuni	Particolari	Deboli
	Categorie degli interessati		

Nella tabella 2 si incrocia il valore del *ranking di attenzione* determinato nella tabella 1 con la numerosità degli interessati coinvolti andando a determinare complessivamente l'intensità delle

misure di sicurezza da adottare. Si individuano tre livelli Basso, Medio e Alto ed una particolare specificazione per i dati personali sanitari (PHI).

Nel caso di trattamenti che coinvolgono dati sanitari risulta opportuno porsi ulteriori domande circa specifiche esigenze quali la anonimizzazione dei dati, la pseudonimizzazione o la crittografia .

Tabella2: intensità delle misure di sicurezza



L'applicazione di quest'ultima tabella ci indica quale sia il livello della misura di sicurezza (basso, medio, alto e PHI) per quei controlli di sicurezza delle misure di sicurezza che si modificano in presenza di trattamenti di dati personali (PII).

5 Controlli e misure di sicurezza

La scelta delle misure da applicare non può quindi prescindere da una valutazione del "valore" del dato personale (PII) e quindi dalla valutazione del rischio legata al trattamento. Infatti, come descritto dall'art.32 del GDPR ("sicurezza del trattamento"), "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*", è dunque compito del titolare del trattamento e del responsabile del trattamento individuare le misure di sicurezza idonee a garantire il livello di sicurezza adeguato al rischio. Sempre nell'art 32 sono indicate alcune misure che potrebbero essere adottate dal titolare e dal responsabile del trattamento in fase di implementazione delle contromisure come la pseudonimizzazione e la cifratura dei dati personali, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Tale elenco è da considerarsi un elenco esemplificativo e non esaustivo in quanto l'individuazione delle altre misure di sicurezza deve essere effettuata in base al contesto in cui queste vengono implementate.

Per quanto riguarda le misure da mettere in atto, il GDPR distingue due macro-categorie o aree: misure organizzative e misure tecniche.

5.1. Misure organizzative

Obiettivo delle misure organizzative è quello di definire e gestire raccomandazioni organizzative (politiche, linee guida, procedure, disciplinari, contratti con i fornitori, ecc.) che regolano le azioni e le attività garantendo un adeguato livello di sicurezza. Misure di sicurezza organizzativa sono ad esempio misure che individuano ruoli e responsabilità, promuovono la consapevolezza e la formazione in ambito cybersecurity, definiscono lo scopo, gli obiettivi, le finalità e gli strumenti per l'attività di audit ,ecc.
Oltre alla documentazione esplicitamente richiesta dalla normativa (registro dei trattamenti, registro degli incidenti, DPIA, …), un'organizzazione dovrebbe quindi sviluppare documenti allo scopo di dimostrare la propria conformità al GDPR come policy e procedure, documentazione tecnica in ambito IT, log, ecc. Per l'individuazione dei documenti da sviluppare l'organizzazione può, oltre a seguire gli obblighi previsti dal GDPR, fare riferimento alle best practice indicate dagli standard di certificazione internazionali, come la norma ISO/IEC27001, (ad es. politica per la gestione della sicurezza, procedura di analisi e trattamento dei rischi, procedura per gli accessi logici, procedura di configurazione apparati di rete perimetrali, disciplinare per gli amministratori di sistema, procedura sistemi di backup, procedure di auditing, ecc.)

5.2. Misure tecniche

Come già accennato il GDPR non fornisce esplicitamente un elenco esaustivo delle misure di sicurezza da adottare ma, al fine di agevolare il compito dei titolari e dei responsabili del trattamento dei dati, raccomanda l'uso di schemi di certificazione per fornire la necessaria garanzia che il Titolare sta gestendo efficacemente i rischi relativi alla sicurezza dei dati come suggerito all'articolo 24, in merito all'adesione ai codici di condotta e alle certificazioni approvate.

Tra gli standard di sicurezza dell'informazione, ad esempio, la ISO/IEC 27001 fornisce un elenco di controlli e presenta molti requisiti e principi simili a quelli delineati dalla GDPR. Ad esempio il concetto di "riservatezza, integrità e disponibilità" richiamato dall'articolo 32 del GDPR è un aspetto centrale all'interno dello standard ISO/IEC 27001; anche la valutazione del rischio è un approccio richiamato sia dal GDPR che dalla ISO/IEC 27001. Altri punti in comune sia al GDPR che alla ISO/IEC 27001 sono la notifica di una violazione dei dati personali (data breach) oppure la gestione dei fornitori dove nell'articolo 28 del GDPR si richiede che i rapporti siano vincolati da accordi allo scopo di garantire il rispetto dei requisiti del regolamento stesso. La ISO/IEC 27001 richiede, infatti, che le organizzazioni assicurino che i processi affidati all'esterno siano identificati e tenuti sotto controllo e fornisce una guida sulle relazioni, il controllo e monitoraggio dei fornitori stessi.

Per quanto riguarda le misure di sicurezza, la ISO/IEC 27001 all'interno dell'allegato A identifica un elenco di misure da adottare per contrastare e/o mitigare i rischi di perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trattati. In particolare, l'elenco prevede 114 controlli, divise in 35 categorie di sicurezza, contenute a sua volta in 14 aree che coprono l'intera gestione della sicurezza delle informazioni:

- Politiche per la sicurezza delle informazioni(A5)
- Organizzazione della sicurezza delle informazioni(A6)
- Sicurezza delle risorse umane (A7)
- Gestione delle risorse(A8)
- Controllo dell'accesso(A9)
- Crittografia(A10)
- Sicurezza fisica e ambientale(A11)
- Sicurezza delle operazioni(A12)
- Sicurezza delle comunicazioni(A13)
- Acquisizione, sviluppo e manutenzione dei sistemi(A14))
- Rapporti con i fornitori(A15)
- Gestione degli incidenti relativi alla sicurezza delle informazioni(A16)
- Aspetti di sicurezza delle informazioni nella gestione della continuità(A17)
- Conformità(A18)

Per ogni categoria di controllo, la norma ISO/IEC 27001 individua un obiettivo di controllo e uno o più controlli (contromisure) che possono essere applicati per raggiungere l'obiettivo di controllo. Ad esempio per l'area di controllo "A.13.1 Gestione della sicurezza della rete" vengono individuati i seguenti controlli:

A.13.1 Gestione della sicurezza della rete		
Obiettivo: Assicurare la protezione delle informazioni nelle reti e nelle strutture per l'elaborazione delle informazioni a loro supporto.		
A.13.1.1	Controlli di rete	*Controllo* Le reti dovrebbero essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
A.13.1.2	Sicurezza dei servizi di rete	*Controllo* I meccanismi di sicurezza, i livelli di servizio e i requisiti di gestione di tutti i servizi di rete

		dovrebbero essere identificati e inclusi negli accordi sui livelli di servizio relativi alla rete, indipendentemente dal fatto che tali servizi siano forniti dall'interno o siano affidati all'esterno.
A.13.1.3	Segregazione delle reti	*Controllo* Nelle reti si dovrebbero segregare gruppi di servizi, di utenti e di sistemi informativi.

Per la scelta dei controlli di sicurezza descritti nell'allegato A della ISO/IEC 27001, il titolare del trattamento e il responsabile del trattamento possono fare riferimento alla norma ISO/IEC27002 che fornisce le "best practices" per la scelta dei controlli nel processo di attuazione di un sistema di gestione per la sicurezza delle informazioni basato sulla ISO/IEC 27001.
La norma ISO/IEC 27002 fornisce, per ogni controllo, una guida attuativa che riporta informazioni più dettagliate per supportare l'attuazione del controllo e il raggiungimento degli obiettivi di controllo. La guida comunque non può risultare completamente attinente o sufficiente in tutte le situazioni e potrebbe non soddisfare i requisiti specifici di controllo dell'organizzazione.
Di seguito, come esempio, viene riportata la guida attuativa per la categoria" Gestione della sicurezza della rete (13.1)" dell'area di controllo "Sicurezza delle comunicazioni(A13)". Per una descrizione completa dei controlli si rimanda alla documentazione ISO.

13	**SICUREZZA DELLE COMUNICAZIONI**
13.1	**Gestione della sicurezza della rete**
13.1.1	**Controlli di rete**
	Controllo
	Le reti dovrebbero essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni
	Guida Attuativa
	Dovrebbero essere attuati controlli per assicurare la sicurezza delle informazioni nelle reti e la protezione dei servizi ad esse relativi dagli accessi non autorizzati. Nello specifico dovrebbero essere considerati i seguenti punti:
	a) dovrebbero essere stabilite le responsabilità e le procedure per la gestione delle apparecchiature dirette.
	b) le responsabilità operative per le reti dovrebbero essere separate dove appropriato da quelle dei sistemi.
	c) dovrebbero essere stabiliti controlli speciali per salvaguardare la riservatezza e l'integrità dei dati in transito su reti pubbliche o su reti wireless e proteggere i sistemi e le applicazioni collegate (vedere punti 10 e 13.2)
	d) dovrebbero essere attive un'adeguata raccolta di log e un monitoraggio che potrebbero influenzare la sicurezza delle informazioni o essere ad essa pertinenti.
	e) le attività di gestione dovrebbero essere strettamente coordinate sia per ottimizzare il servizio reso all'organizzazione sia per assicurare che i controlli siano applicati in modo coerente sulle strutture per l'elaborazione delle informazioni.
	f) i sistemi dovrebbero essere autenticati sulla rete.
	g) la connessione dei sistemi alla rete dovrebbe essere limitata.

	Altre informazioni:
	Informazioni aggiuntive sulla sicurezza della rete possono essere trovate nella ISO/IEC 27033 [15] [16] [17] [18] [19]

5.3. Lo standard ISO/IEC 27701

Nell'agosto del 2019 è stata pubblicata la norma ISO/IEC 27701 che specifica i requisiti e fornisce una guida per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione delle informazioni sulla privacy (PIMS) estendendo i requisiti delle norme ISO / IEC 27001 e ISO / IEC 27002 per la gestione della privacy nel contesto dell'organizzazione. Questa norma pertanto fornisce una guida per le organizzazioni sia pubbliche che private che operano come Titolari e/o responsabili del trattamento.

La norma ISO/IEC 27701 contiene le seguenti sezioni:

1. Il paragrafo 5 fornisce una guida specifica per PIMS e altre informazioni riguardanti i controlli di sicurezza delle informazioni in ISO / IEC 27001 alle organizzazioni che intendono operare come Titolare o Responsabile del trattamento.
2. Il paragrafo 6 fornisce una guida specifica per PIMS e altre informazioni riguardanti i controlli di sicurezza delle informazioni in ISO / IEC 27002 alle organizzazioni che intendono operare come Titolare o Responsabile del trattamento.
3. Il paragrafo 7 fornisce una guida aggiuntiva rispetto alle indicazioni della ISO/IEC 27002 per le organizzazioni che operano come Titolare del trattamento (PII Controllers)
4. Il paragrafo 8 fornisce una guida aggiuntiva rispetto alle indicazioni della ISO/IEC 27002 per le organizzazioni che operano come Responsabile del trattamento (PII Processors).

La norma SIO/IEC 27701 inoltre presenta i seguenti allegati:

1. Allegato A: contiene i controlli per un PIMS che opera come titolare del trattamento (PII Controllers)
2. Allegato B: contiene i controlli per un PIMS che opera come responsabile del trattamento (PII Processors)
3. Allegato C: mappatura alla norma ISO/IEC 29100 (Information technology - Security Techniques Privacy Framework)
4. Allegato D: fornisce la mappatura con il GDPR.
5. Allegato E: fornisce la mappatura con la norma ISO/IEC 27018 e ISO/IEC 29151
6. Allegato F: descrive come applicare la norma ISO/IEC 27701 alla ISO/IEC 27001 e alla ISO/IEC 27002

Di seguito, come esempio, sono riportate le estensioni di controllo introdotte dalla norma ISO/IEC 27701 per il controllo "Sicurezza delle comunicazioni(A13)":

Rif. ISO/IEC27701	**Rif. ISO/IEC 27001 (All. A)**	**Titolo (ISO/IEC27001/27002)**	**Estensione del controllo (ISO/IEC27701)**

6.10.1	**A.13.1**	**Gestione della sicurezza della rete**	
6.10.1.1	A.13.1.1	Controlli di rete	Nessuna estensione
6.10.1.2	A.13.1.2	Sicurezza dei servizi di rete	Nessuna estensione
6.10.1.3	A.13.1.3	Segregazione delle reti	Nessuna estensione
6.10.2	**A.13.2**	**Trasferimento delle Informazioni**	
6.10.2.1	A.13.2.1	Politiche e procedure per il trasferimento delle informazioni	L'organizzazione dovrebbe prendere in considerazione le procedure per garantire che le regole relative al trattamento del PII siano applicate all'interno e all'esterno del sistema, ove applicabile.
6.10.2.2	A.13.2.2	Accordi per il trasferimento	Nessuna estensione
6.10.2.3	A.13.2.3	Messaggistica elettronica	Nessuna estensione
6.10.2.4	A.13.2.4	Accordi di riservatezza o di non divulgazione	L'organizzazione dovrebbe garantire che le persone che operano sotto il suo controllo con accesso a Pll siano soggette a un obbligo di riservatezza. L'accordo di riservatezza, sia esso parte di un contratto o separato, dovrebbe specificare il periodo di tempo in cui gli obblighi devono essere rispettati. Quando l'organizzazione è un responsabile del trattamento dei dati, un accordo di riservatezza, in qualsiasi forma, tra l'organizzazione, i suoi dipendenti e i suoi agenti dovrebbe garantire che i dipendenti e gli agenti rispettino la politica e le procedure relative alla gestione e alla protezione dei dati.

Per la descrizione completa dei controlli della ISO/IEC 27701 e delle estensioni dei controlli rispetto alla norma ISO/IEC 27001 e 27002 si rimanda alla documentazione “ISO/IEC 27701:2019 – Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines”.

Un altro strumento molto utile a valutare i controlli di sicurezza è la Pubblicazione Speciale 800-53 emessa dal "National Institute of Standards and Technology" (NIST), il NIST 800-53SP. Tale pubblicazione risulta essere un catalogo di gruppi o famiglie di controlli della sicurezza e della privacy che coprono aree come il controllo degli accessi, la formazione sulla consapevolezza della sicurezza, le valutazioni formali del rischio, la risposta agli incidenti o il monitoraggio continuo a supporto della gestione del rischio organizzativo.
Ogni famiglia contiene controlli di sicurezza relativi ad un determinato argomento o ambito che comprendono aspetti di governance, processi, azioni dei singoli individui, meccanismi automatizzati e implementati da sistemi/dispositivi.
Di seguito riportiamo le famiglie della versione 4 del documento 800-53SP (al momento della stesura di questo documento, il NIST sta lavorando alla versione 5 che è ancora in versione draft):

ID	Famiglia	ID	Famiglia
AC	Controllo degli Accessi	MP	Supporti di memorizzazione
AT	Sensibilizzazione e Formazione	PE	Protezione Fisica e ambientale
AU	Audit e Accountability	PL	Planning
CA	Valutazione della scurezza e autorizzazione	PS	Sicurezza del Personale
CM	Gestione dei cambiamenti	RA	Valutazione del rischio
CP	Piano di emergenza	SA	Acquisizione di sistemi e servizi
IA	Identificazione e Autenticazione	SC	Protezione delle comunicazioni e dei sistemi
IR	Risposte agli Incidenti (Gestione del rischio)	SI	Integrità delle informazioni e dei sistemi
MA	Manutenzione	PM	Program Management

I controlli di sicurezza di ogni famiglia presentano un alto grado di dettaglio e personalizzazione e permettono una più facile correlazione con la classificazione, basso-medio-alto, dei dati trattati.
Ogni controllo infatti è formato dalle seguenti sezioni:
- Controllo(*control)*: Questa sezione descrive il controllo di sicurezza da implementare.
- Guida supplementare (*supplemental guidance)*: Fornisce ulteriori informazioni e linee guide per l'implementazione del controllo
- Controlli migliorativi *(Control Enhancements:)*: Questa sezione contiene ulteriori controlli di sicurezza da implementare
- Riferimenti *(References):* Contiene i riferimenti ad altri documenti, leggi, linee guida.
- Priorità e livello di applicazione (*Priority and Baseline Allocation*): Questa sezione indica il livello di priorità del controllo che permette di individuare l'ordine con cui implementare i controlli della stessa famiglia. Inoltre il livello di applicazione permette di correlare il controllo con il livello di classificazione (LOW/Basso, MOD/Medio, HIGH/Alto) dei dati trattati.
Per alcuni controlli, il NIST fornisce un ulteriore flessibilità consentendo alle organizzazioni di definire il valore di specifici parametri (nel documento questi parametri sono racchiusi tra parantesi quadre) dando quindi la possibilità al titolare e al responsabile del trattamento di adattare tali controlli in base ai requisiti di sicurezza e protezione dei dati trattai.
Di seguito, come esempio, riportiamo la descrizione completa del controllo "AU-4 Audit storage capacty" mentre per una descrizione completa dei controlli si rimanda all' "Allegato F" al documento del NIST (800-53SP rev.4).

AU-4 Capacità di memorizzazione della registrazione(log) delle attività

Controllo: L'organizzazione dimensiona la capacità di memorizzazione registrazione(log) delle attività in base a [*i requisiti di archiviazione dei log di controllo definiti dall'organizzazione*].

Guida supplementare: L'organizzazione nel dimensionare la capacità di memorizzazione della registrazione(log) delle attività nei sistemi informativi deve considerare quali sono le informazioni e gli eventi che deve registrare e quali operazioni deve effettuare su tali registrazioni. Un adeguato dimensionamento della capacità di archiviazione dei log permette di ridurre la probabilità che tale capacità venga superata e quindi di ridurre il rischio di una potenziale perdita dei dati. Controlli NIST correlati: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4

Controlli migliorativi:
(1) Trasferimento dei log a supporti di memorizzazione alternativi:
Il sistema informativo scarica le registrazioni (log) delle attività *[parametro da personalizzare: frequenza definita dall'organizzazione]* su un sistema o supporto diverso rispetto al sistema da controllare.

Riferimenti: Nessuno

Priorità e Livello di applicazione:

P1	**LOW** AU-4	**MOD** AU-4	**HIGH** AU-4

L'allegato H del documento del NIST, inoltre, fornisce una mappatura con i controlli di sicurezza dello standard ISO/IEC 27001:2013 permettendo al titolare e al responsabile del trattamento di integrare i framework e standard come la ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27701 con le misure di sicurezza del NIST che, come abbiamo già detto, si adattano ai livelli di classificazione (Basso, Medio, Alto) dei dati trattati secondo la metodologia illustrata nel paragrafo precedente.

5.4. NIST Privacy Overlay

Il NIST ha osservato che "il trattamento dei dati personali (PII) è distinto da altri tipi di dati perché deve essere non solo protetto, ma anche raccolto, mantenuto e diffuso in conformità con le normative in ambito protezione dei dati" e, come mostrato anche nella tabella 2 "Intensità delle misure di sicurezza", i dati personali non hanno tutti lo stesso "valore" ma i dati personali con valore più alto richiedono misure di sicurezza più stringenti.
Nel documento NIST Privacy Overlay vengono infatti individuati alcuni controlli di sicurezza dal documento NIST 800-53SP che richiedono particolare attenzione quando vengono trattati dati personali (PII) o dati sanitari (PHI); ad esempio per il gruppo AC-2 (Gestione degli account) i controlli da considerare sono:

Controllo	**Nome del controllo**
AC-2	Account management
AC-2(8)	Dynamic account creation

AC-2(9)	Restrictions on use of shared / group accounts
AC-2(13)	Disable accounts for high-risk individuals

Di seguito, viene riportato l'esempio di come il documento NIST Privacy Overlay può essere applicato alla famiglia AC-2 dove viene indicato:
- La Motivazione per la quale quel controllo risulta indispensabile per la protezione di PII,
- L' estensione del controllo per i diversi livelli (B, M, A) e per ciascuno di questi i valori dei parametri che li caratterizzano,
- L'indicazione degli altri controlli correlati.

Per una descrizione completa dei controlli si rimanda al documento Privacy Overlay e al NIST Special Publication 800-53 ().

AC-2 Account management: Gestione degli account

Motivazione
La gestione degli accessi alle applicazioni e sistemi IT, attraverso credenziali attribuite a persone fisiche (Account) è una funzione fondamentale per lo sviluppo e l'implementazione di un quadro di controllo dell'accesso adeguato alle informazioni con particolare riferimento a quelle personali (PII).
La gestione dell'account è una funzione fondamentale per lo sviluppo e l'implementazione di un quadro di controllo dell'accesso adeguato alle informazioni (PII) contenute nei sistemi e nelle applicazioni. Se implementato in modo efficace, il framework di controllo degli accessi fornisce i costrutti necessari per il controllo dell'accesso alle PII, limitando la divulgazione dei record sugli individui solo ai sistemi e agli utenti dell'applicazione che hanno bisogno delle informazioni per svolgere le loro funzioni lavorative. Lo scopo di questa guida è stabilire i requisiti per l'accesso degli utenti a ad informazioni di personale di tipo sanitario o giudiziario (PHI) e informazioni personali (PII).

Estensione del controllo: livello Basso

Vietato l'uso di account guest, anonimi e condivisi per fornire accesso alle informazioni personali (PII).
Deve essere notificato al gestore degli account *entro un periodo massimo* ***di due giorni*** lavorativi dall'organizzazione quando non sono più necessari account temporanei o quando gli utenti del sistema informativo vengono chiusi o trasferiti o l'utilizzo del sistema di informazioni o la necessità di conoscere/la necessità di condividere le modifiche. Prima di concedere l'accesso alle informazioni personali, gli utenti dimostrano la necessità delle informazioni personali nell'esercizio delle loro funzioni.
Tale esigenza viene certificata dalla individuazione delle persone fisiche a cui vengono associati degli account quali ***autorizzati*** nel registro dei trattamenti, in riferimento agli specifici trattamenti.

Valore dei parametri specifici

a) Gestire gli account tenendo presente che ogni utente debba completare e superare almeno una volta l'anno un percorso formativo in materia di data protection. In assenza di questo l'account deve essere disabilitato.
b) Processo di revisione degli account per la compliance con le indicazioni che possono variare nel tempo almeno annualmente.

Estensione di controllo: livello Medio e Alto

Applicare l'estensione di controllo del livello Basso. La individuazione degli account deve seguire un principio e una granularità che consenta di collegare ad un account solo la quantità minima di informazioni personali necessarie agli utenti per svolgere le proprie funzioni.

Valore dei parametri specifici

c) Come livello inferiore
d) Processo di revisione degli account per la compliance con le indicazioni che possono variare nel tempo, *annualmente per gli utenti generali* e *quadrimestrale per gli account privilegiati* ad esempio gli amministratori di sistema (es. DB amministrator, Account manager, ecc.)

Controlli correlati:

AC-16, AC-3

6. Un Primo Passo

Quanto descritto nel capitolo precedente rappresenta un obiettivo a cui tendere che dovrà essere raggiunto per passi.
Un primo aspetto, quello dalla adesione formale alla messa in atto di processi organizzativi così come definiti dallo standard ISO/IEC 27001e 27701 sarà soddisfatto dall'approvazione di un Framework per la sicurezza della Regione Toscana.
Come è stato precedentemente descritto lo Standard ISO/IEC 27xxx non entra nel merito specifico dei dati trattati ed in particolare dei dati personali, mentre il NIST individua a seconda della categorie di dati personali trattati, dei livelli differenti (basso, medio, alto e sanità) nella definizione delle misure e dei controlli di sicurezza da adottare.
Il NIST presenta una granularità molto fina nella individuazione dei controlli e pertanto, una sua adesione all'interno dell'organizzazione regionale, dovrebbe essere preceduta da un lavoro molto lungo ed accurato.
Al fine di fornire una linea guida metodologica e una adeguata, seppur non esaustiva, indicazione circa le misure di sicurezza e relativi controlli, da adottare, proseguiremo con la granularità delle "famiglie" individuata nel documento Data Protection Policy per le misure di sicurezza.
Le misure di sicurezza, nel documento di Data Protection Policy, secondo un principio di semplicità operativa nella prima attuazione del GDPR, sono state rappresentate secondo le seguenti famiglie che costituiscono una definizione con granularità maggiore delle famiglie e dei controlli ISO/IEC e soprattutto di quelli del NIST, ma a che a questi standard possono essere riportate:

1. Sicurezza delle Identità
2. Sicurezza dei Dispositivi di accesso
3. Sicurezza delle Reti
4. Sicurezza dei Sistemi
5. Sicurezza Organizzativa
6. Sicurezza Fisica
7. Disaster Recovery e continuità operativa
8. Misure specifiche per la data protection di dati particolari

Si rimanda al documento Data Protection Policy – Linee guida sulle misure di sicurezza, per la loro descrizione.

6.1. Disegno architetturale

Una prima indicazione per un approccio Data Protection by Design riguarda la progettazione o la ristrutturazione delle architetture IT che andranno ad organizzare le diversi componenti in modo coerente con le valutazioni e le scelte che dovranno essere fatte in merito alla sicurezza adeguata ai dati personali trattati.
Pertanto, il disegno dell'architettura infrastrutturale complessiva di un sistema deve mettere in evidenza le sue caratteristiche che si devono mappare con il livello di sicurezza adottato per le diverse componenti in relazione ai controlli delle famiglie delle misure di sicurezza.
Attraverso il disegno architetturale del sistema che si progetta o che si gestisce, si possono andare a definire:

a) **i contesti,** ad esempio quello organizzativo che rappresenta la collocazione fisica dei sistemi o il contesto tecnologico;
b) **gli ambiti,** che per il contesto organizzativo possono essere locali a maggiore o minore sicurezza, e che per quello tecnologico possono essere "sotto reti"(comprensive dei sistemi) soggette a diversi meccanismi e attività di sicurezza;
c) **i sotto-ambiti,** che nel caso di contesti tecnologici possono essere particolari sistemi di gestione di basi di dati o altro.

Nella seguente tabella si rappresenta il collegamento fra i contesti e i relativi ambiti e sotto-ambiti e le "famiglie" delle misure di sicurezza per le quali occorre produrre "i controlli.

Contesto applicazione	***Ambiti***	***Sotto-ambiti***	***Controlli da produrre***
Contesto Organizzativo (es. sistema dei locali fisici di un data center)			***1. Sicurezza Organizzativa*** ***2. Sicurezza Fisica***
Contesto tecnologico Generale (es. un intero data center)			***1. Sicurezza dei sistemi*** ***2. Sicurezza delle Reti*** ***3. Sicurezza dei dispositivi***
	Contesto tecnologico Specifico (es. una sotto rete dedicata ad uno specifico settore di attività)		***1. Eredita misure di sicurezza del livello gerarchico superiore.*** ***2. Sicurezza delle identità*** ***3. Rafforzamento delle misure di sicurezza ereditate*** 4. ***Disaster recovery e continuità operativa***

Contesto applicazione	*Ambiti*	*Sotto-ambiti*	*Controlli da produrre*
		Sistema di basi di dati (es. basi dati sanitarie)	***1. Eredita misure di sicurezza del livello gerarchico superiore.*** ***2. Rafforzamento delle misure di sicurezza ereditate*** ***3. Misure specifiche per la data protecion di dati particolari***

Gli Asset (applicazioni, server, apparati di rete, ecc..), costituiranno quindi delle componenti del sistema generale che andranno ad essere definiti e collocati all'interno dei diversi contesti e relativi ambiti e sotto ambiti e contribuiranno con le loro specifiche a determinarne la sicurezza. Definire la sicurezza per contesto, ambiti e sotto-ambiti semplifica e rende quindi più sicuro anche l'effettuarsi delle attività di corredo quali il monitoraggio, la verifica, gli interventi migliorativi, la problem determination ecc.
Avremo pertanto contesti e loro articolazioni che potremo etichettare con valori garantiti di sicurezza in relazione ai controlli e alle misure che saranno adottate andando a determinarne il livello basso, medio, alto e specifico per dati relativi alla salute.
Questo consentirà di individuare il contesto, l'ambito e il sotto ambito nel quale andare a collocare applicazioni e basi di dati sulla base del valore dei dati personali trattati.

7. Famiglie e controlli – primo step

In attesa di disporre di uno studio di applicazione di dettaglio degli standard NIST, che nella presente linea guida, indichiamo come, ad oggi, il modello da seguire nell'individuare i controlli di sicurezza per la data protection, offriamo un primo step, uno schema di ragionamento, che, partendo dalle famiglie individuate nella data protection policy, vada ad individuare quei controlli che maggiormente si riferiscono al tema della protezione dei dati personali (PII).
Si suggerisce di usare la metodologia qui illustrata e le relative tabelle in tutte le fasi che riguardano il tema della sicurezza con particolare riferimento a:

a) progettazione di un sistema informativo,
b) definizione dei requirements di sicurezza in una procedura di acquisto di servizi IT,
c) definizione degli elementi che debbono essere descritti da parte di partecipanti a procedure di acquisto,
d) rilevazione (assessment) sulla sicurezza di sistemi esistenti,
e) determinazione degli interventi tesi a migliorare i livelli di sicurezza.

Nel seguito indichiamo: per ogni famiglia di misure di sicurezza così come definite nella Data Protection Policy:

a) i controlli di sicurezza,

b) i parametri di misura di quei controlli, che possono essere la presenza o meno di un documento descrittivo e il suo riferimento, la presenza o meno di specifiche componenti di sistema, la frequenza di svolgimento di attività, ecc.
c) la indicazione di specifici “livelli di sicurezza” per i quali devono essere esplicitati e valorizzati i parametri.

In questo primo step si sono evidenziate solo quelle “famiglie” che riguardano principalmente il tema della Data Protection di PII, consapevoli che questo rappresenta solo un primo passo di un percorso non breve e che procederà per approssimazioni successive, prima di giungere ad una sua definitiva formalizzazione che sarebbe opportuno avvenisse almeno a livello nazionale.

7.1. Famiglia: Sicurezza delle identità

Controlli	**Parametri**	**basso**	**medio**	**alto**	**sanità**
Processo di provisioning e deprovisionig delle credenziali utente.	Documento				
Verifica del mantenimento del diritto sulle credenziali.	Documento. Sistema utilizzato. Frequenza del controllo.				
Processo di provisioning e deprovisionig dei privilegi per gli amministratori di sistema, e collegamento con l’elenco degli amministratori di sistema.	Documento				
Verifica del mantenimento del diritto dei privilegi, e rispetto del principio di Duty Separation	Documento. Sistema utilizzato. Frequenza del controllo.				
Sistemi di autenticazione (utente passwd, due fattori, smart card, spid ..) utilizzati.	Indicazione del metodo. Indicazione degli strumenti tecnologici				
Sistema di identificazione e accesso con indicazione dei sistemi di invocazione delle applicazioni e passaggio dei parametri (identificazione, ruolo, profilo), con indicazione delle misure di sicurezza adottate.	Documento.				
Recovery e Restart del sistema complessivo della gestione identità ruoli e proifili	Tempo di ripristino della componente e del servizio, sullo stesso sistema e su altri sistemi.				
Descrizione dei sistema	Documento. Livelli di alta				

complessivo (HW e SW) di gestione delle identità dei ruoli e dei profili.	affidabilità, Livelli di alta disponibilità, Parametri MTTR, MTBF, ecc..				
Business continuity	Tempo di disservizio.				
File di log	Documento. Frequenza. Tempo di mantenimento				
Aggiornamento delle release o patch	Frequenza.				
sistema di intrusion detection	Documento.				
sistema di verifica di congruenza fra gli accessi effettuati con gli autorizzati nel registro trattamenti	Documento. Frequenza della verifica.				
Sistema di congruenza fra gli accessi effettuati e l'elenco degli amministratori di sistema	Documento. Frequenza della verifica.				
Modalità di restituzione dei dati	Documento. Formato dei dati. Tempo intercorrente dalla richiesta.				
Performance del sistema di Identificazione ruolo e profilo.	Tempo medio di invocazione dell'applicazione. (di sistema e percepita dall'utente)				
Sistemi di rilevazione della percezione dell'utente	Documento. Report e Frequenza del Report.				
Sistemi di identificazione per l'accesso ai locali	Documento				
Sistemi di identificazione per l'accesso agli apparati	Documento				
Livelli di identificazione e autorizzazione per l'accesso alle risorse di rete (cartelle di rete, ecc..)	Documento.				
Sistemi di identificazione per l'accesso a dispositivi fissi e mobili (PC, Tablet, SmartPhone ecc..)	Documento. Tipologie e livelli di sicurezza.				

7.2. Famiglia: Sicurezza dei dispositivi di accesso

Controlli	***parametri***	***basso***	***medio***	***alto***	***sanità***
Restrizioni di uso, modalità di connessione per ogni tipo di dispositivo,	documento				

compresa la interoperabilità fra sistemi					
Modalità di monitoraggio e controllo delle connessioni	Documenti. Metodi				
Metodi di sicurezza delle connessioni (Criptografia, VPN, certificati, ecc..)	Metodo.				
Sistemi di identificazione del dispositivo e associazione con l'utente e relativi profili.	Documento.				
Metodi di comunicazione fra sistemi informativi diversi, gestione dei profili e diritti sulle operazioni. (certificati,...)	Documento.				
Tecniche di controllo sulle operazioni che possono avvenire attraverso connessioni. (es. controllare quantità e qualità dei dati acceduti/scaricati)	Documento.				
Rilevazione della liceità di operazioni effettuate sui dati nel caso particolare di dati classificati personali e relativo livello di valore	Documento.				
Evitare/consentire la memorizzazione in locale su dispositivi mobili o PC di categorie di dati personali	Documento.				
Gestione degli autorizzati	Documento. Frequenza del controllo				
Gestione degli amministratori di sistema	Documento. Frequenza del controllo				
Metodi di audit	Documento				
Attività di audi	Frequenza				
Tecniche e metodi di condivisione di informazioni. (File sharing, servizi in Cloud, ecc.)	Documento				
Tecniche di sicurezza nella condivisione di informazioni	Documento.				

Metodi e Strumenti di configurazione dei dispositivi di accesso.	Documento				
Attività di audit sulle configurazioni	Documento. Frequenza.				

7.3. Famiglia: Sicurezza delle reti

Controlli	parametri	basso	medio	alto	sanità
Processo di gestione delle infrastrutture di rete.	Documento				
Descrizione dell'architettura di rete	Documento.				
Caratteristiche delle funzionalità di sicurezza degli apparati attivi	Documento				
Sistemi e attività di intrusion detection.	Documento. Report. Frequenza.				
Sistemi di monitoraggio	Documento. Frequenza				
Sistema di audit delle performance e report	Documento. Report. Frequenza.				
Controllo amministratori di sistema	Documento. Frequenza				
Formazione degli amministratori di sistema	Documento. Frequenza				
Garanzie sulla continuità operativa	Documento. Indicatori di performance e continuità.				
Sicurezza fisica degli apparati	documento				
Rilevamento e gestione degli incidenti	Documento. Tempi di conduzione dell'incidente.				
Affidabilità degli apparati/Sottorete	Indicatori di performance e continuità (MTTR, MTBF, ecc..)				
Elenco minacce e contromisure, e suo aggiornamento	Documento. Frequenza.				
Gestione, salvataggio e controllo delle configurazioni degli apparati	Documento. Frequenza				

7.4. Famiglia: Sicurezza dei Sistemi

Controlli	*parametri*	*basso*	*medio*	*alto*	*sanità*

Descrizione: a) della architettura: fisica, logica b) della collocazione dei dati con particolare riferimento ai dati personali, c) dei meccanismi di catalogazione delle risorse, d) della classificazione dei dati.	Documento				
Individuazione delle principali minacce, dei rischi e delle contromisure.	Documento				
Revisione delle minacce, rischi e contromisure	Documento. Report. Frequenza				
Processo di gestione dei sistemi dove per sistemi si intendono: a) le risorse computazionali, b) le risorse di storage, c) le risorse di gestione dei dati (DB, file system, ecc.) d) le risorse applicative (applicazioni) che realizzano i trattamenti dati.	Documento				
Sicurezza fisica ed operativa delle diverse tipologie di risorse (modalità di accesso fisico e operativo ai server e alle diverse componenti operative). Monitoraggio.	Documento. Frequenza dei controlli.				
Organizzazione dei privilegi degli amministratori di sistema per le diverse componenti. Sistemi e attività di controllo	Documento. Frequenza dei controlli.				

Descrizione dei meccanismi di alta affidabilità e alta disponibilità delle risorse fisiche (computazionali e di storage) Monitoraggio.	Documento. Report. Frequenza controlli.				
Descrizione dei sistemi di recovery e restart delle componenti operative e delle verifiche.	Documento. Frequenza delle verifiche (test)				
Meccanismi intrinseci di sicurezza rispetto alle diverse tipologie di risorse, verifica e aggiornamento.	Documento. Frequenza verifiche.				
Descrizione dei sistemi di business continuity sulle diverse risorse, monitoraggio e verifiche.	Documento, Report. Frequenza.				
Formazione del personale addetto alla gestione	Frequenza				
Auditing delle performance e della sicurezza per le diverse tipologie di risorse	Report. Frequenza.				
Risk assessment sulle diverse tipologie diverse tipologie di risorse	Documento. Frequenza				
Descrizione del livello di portabilità e delle misure di no lock in	Documento.				
Elenco delle principali minacce e delle contromisure adottate per le diverse tipologie di risorse	Documento. Frequenza di revisione.				
Tecniche di pseudonimizzazione	Documento.				
Tecniche di crittografia	Documento				
Gestione degli incidenti	Documento. Tempi di individuazione del problema. Tempi di attivazione misure intermedie per la riduzione del rischio. Tempi di dispiegamento della soluzione individuata				

Un primo e concreto esempio di verifica e implementazione di questo modello di rappresentazione della sicurezza di un sistema potrebbe essere applicazione al contratto SCT.

8. Riferimenti

- ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

- ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls

- ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines

- UNI CEI EN ISO/IEC 27001:2017 – Information technology – Security techniques – Information security management systems – Requirements

- UNI CEI EN ISO/IEC 27002:2017 – Information technology – Security techniques – Code of practice for information security controls

- UNI CEI ISO/IEC 27002:2014 – Tecnologie Informatiche – Tecniche per la sicurezza – Raccolta di prassi sui controlli per la sicurezza delle informazioni

- NIST Special Publication 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organization.

- Privacy Overlay – Attachment 6 to Appendix F (Formerly Appendix K), CNSS Published Overlay