ISTITUTO COMPRENSIVO
"C. SALUTATI - A. CAVALCANTI"
Piazza A. Moro, 1 – 51011 Borgo a Buggiano (PT)
C.F.: 81003470473 - tel. 0572 - 32018
ptic81900g@istruzione.it – ptic81900g@pec.istruzione.it www.istitutosalutaticavalcanti.it

I.C.S. - "SALUTATI - CAVALCANTI"-BUGGIANO
Prot. 0002627 del 05/07/2023
III (Uscita)

LINEE GUIDA SVILUPPO SOFTWARE

Sommario

1. Introduzione 3
1.1 Scopo e Riferimenti normativi 3
2. DEFINIZIONI 4
2.1 GDPR 4
2.2 Relazione 5
3. Specifiche rispetto alle attività di realizzazione del Prodotto 6
3.1 Formazione 6
3.2 Pre-analisi 6
3.3 Miminimizzazione dei dati presenti nell'architettura del Prodotto. 8
3.4 Elementi di Design obbligatori 8
3.5 Testing 11
3.6 Prodotti su storage messi a disposizione dalla Società 11
3.7 Subfornitori e terze parti 12
4. Revisione 12

1. Introduzione

1.1 Scopo e Riferimenti normativi

Ai sensi del Considerando 78 della GDPR, la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del Regolamento. Al fine di poter dimostrare la conformità al testo europeo, devono essere adottate politiche interne deputate ad attuare misure che soddisfino in particolare i principi della **protezione dei dati fin dalla progettazione e della protezione dei dati di default**.

Pertanto, e tenuto conto dello stato dell'arte, i fornitori di software/servizi (*per il prosieguo anche solo "Prodotto"*) che elaborano o comunque trattano dati personali di persone fisiche e/o che incidono sulle misure di sicurezza a presidio di questi, devono tener conto già dalle fasi di progettazione, sviluppo, implementazione, manutenzione e aggiornamento, del diritto alla protezione dei dati personali e dei principi che regolano tutta la materia privacy. E ciò tenendo conto dell'evoluzione tecnologica e del contesto in cui i software/servizi opereranno, con le relative peculiarità, rispetto sia ai dati che ai trattamenti.

Le presenti Linee guida mirano di indicare alla Società alcuni macro temi che devono essere osservati nella realizzazione dei software/servizi destinati al mercato europeo, tenendo conto in primis del principio cardine che guida tutta la GDPR, ossia il principio di accountability[2], e che, senza dettare risoluzioni tassative, **rimette al singolo operatore l'obbligo di dimostrare l'adeguatezza delle misure tecniche ed organizzative implementate** per osservare quanto il Regolamento impone.

Allo scopo, si è tenuto di conto dei seguenti riferimenti:

a. GDPR - Regolamento UE 2016/679;
b. Principi di Privacy by Design e Privacy by Default
    - Approccio proattivo non reattivo, prevenire per correggere: ossia anticipare e prevenire gli eventi invasivi/lesivi della privacy prima che essi accadano,
    - Privacy come impostazione di default: realizzare il massimo livello di privacy, assicurando che i dati personali sono automaticamente protetti in un qualunque sistema IT o di pratica commerciale,
    - Privacy incorporata nella progettazione,
    - Sicurezza dell'intero ciclo-vita di un sistema e dei dati,
    - Visibilità e trasparenza costante verso l'interessato/utente e centralità dell'utente;
c. WP 29 – Guidelines on personal data breach notification;
d. WP 29 – Parere 5/2014 sulle tecniche di pseudonimizzazione;
e. WP 29 – Guidelines on DPOs;
f. WP 29 – Guidelines on automated individuale decisioni-making and profiling for purpose of GDPR;
g. D.Lgs. 196/2003;
h. Provvedimenti dell'Autorità Garante per la protezione dei dati personali.

Quello che viene richiesto rispetto ai software è di comprovare, sia a livello tecnico che documentale, **come i Principi di Privacy by Design e di Privacy by Default** *(unitamente intesi "PbD"*

[2] *Tenuto 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 della persona fisiche, devono essere attuate misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato*

per il prosieguo) **siano stati applicati al prodotto/servizio sviluppato**, sia *ab initio* che in costanza (p.e. laddove il software venga aggiornato, la normativa muti, o la tecnologia innalzi i suoi standard). Pertanto, la PbD diventa un requisito del software necessario per rispondere alle esigenze normative dettate dal GDPR, nonché un elemento di competitività sul mercato.

2. DEFINIZIONI

2.1 GDPR

Di seguito vengono riportate le definizioni indicate dall'art. 4 del GDPR delle quali bisogna tener conto nella presente Relazione.

«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica 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;

«trattamento»: 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;

«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine

conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

«impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

«gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

«norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

«amministratore si sistema»: le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

2.2 *Relazione*

Prodotto: applicativo, software, servizio commercializzato dalla Società e con impatti sotto il profilo data protection

Utilizzatore: società che commissione il Prodotto, o che lo acquista per utilizzarlo o per commercializzarlo

3. Specifiche rispetto alle attività di realizzazione del Prodotto

3.1 Formazione

L'implementazione dei principi di PbD passa necessariamente dalla consapevolezza dei soggetti deputati a progettare e realizzare il prodotto rispetto ai principi che regolano la materia privacy, nonché dalla conoscenza degli elementi di data protection ed information security.

E' un passaggio essenziale creare cultura su tali temi, ed aumentare le competenze attraverso momenti formativi che siano pratici e funzionali rispetto alle varie fasi del processo produttivo. E' necessario pertanto

1. individuare i soggetti da formare, identificando i dipendenti ed i fornitori che prestano stabilmente i propri servizi in azienda rilevanti rispetto al tema (es. sviluppatori, project owner, product owner, architetti del software ecc.);
2. progettare corsi di formazione su:
    a. gli aspetti di sicurezza informatica,
    b. la data protection law,
    c. le best practices in materia informatica,
    d. gli standard internazionali,
    e. le ISO rilevanti;
3. assegnare la docenza a più professionisti multidisciplinari, affinché siano affrontati con un taglio sia informatico che legale i temi trasversali rispetto al software/servizio;
4. al termine del corso effettuare dei test per valutare lo stato di recepimento degli argomenti esposti;
5. decidere la periodicità del corso, tenendo conto delle novità normative e delle evoluzioni tecniche anche sotto il profilo delle minacce.

3.2 Pre-analisi

Per impostare i requisiti del Prodotto è necessario in prima battuta valutare gli aspetti di seguito indicati. Tali aspetti non devono essere stimati in modo asettico, bensì combinati tra loro con riferimento agli utilizzi cui il software è destinato.

1. Se il software tratta o meno dati personali	
Qualora l'applicativo non tratti dati di persone fisiche *[es. dati aggregati e non disaggregabili, oppure dati non riferibili a persone fisiche]*	Devono essere tenuti in considerazione gli aspetti di sicurezza, ma non quelli privacy
Qualora l'applicativo tratti dati di persone fisiche *[es. nome/cognome, email, codici identificativi, stato di salute, geolocalizzione, immagini ecc.]*	Devono essere tenuti in considerazione gli aspetti di sicurezza, Devono essere tenuti in considerazione anche gli aspetti privacy

2. Quali categorie di dati personali verranno trattati dal software	
Il software tratta solo dati identificativi *[es. nome e cognome, email, telefono]*	Attenzione data protecion: MEDIA
Il software tratta anche dati para-particolati *[es. dati reddituali, patrimoniali od economici di persone fisiche]*	Attenzione data protecion: MEDIO/ALTA
Il software tratta anche dati particolari *[es. dati relativi allo stato di salute, alle convinzioni politiche o religiose]*	Attenzione data protecion: ALTA
Il software tratta anche dati di geolocalizzazione	Attenzione data protecion: ALTA
Il software tratta anche dati biometrici	Attenzione data protecion: ALTISSIMA

3. Finalità dei trattamenti effettuati mediante il software	
Il software effettua trattamenti obbligatori per legge *[es. contabilità e adempimenti fiscali]*	Attenzione data protecion: MEDIA
Il software effettua trattamenti in esubero a quelli essenziali poiché funzionali alla realizzazione degli obiettivi aziendali dell'utilizzatore *[es. CRM, marketing]*	Attenzione data protecion: ALTA
Tramite il software è possibile effettuare attività di profilazione degli interessati	Attenzione data protecion: ALTISSIMA
Tramite il software è possibile prendere decisioni automatizzate che influiscono direttamente sulla sfera giuridica dell'interessato	Attenzione data protecion: ALTISSIMA

4. In quali settori di mercato verrà destinato il software	
Produttivo	Attenzione data protecion: MEDIA
GDO e Multiutility	Attenzione data protecion: MEDIO/ALTA
Pubblico	Attenzione data protecion: MEDIO/ALTA
Farmaceutico/Sanitario	Attenzione data protecion: ALTISSIMA
Assicurativo/Bancario	Attenzione data protecion: ALTISSIMA

3.3 Minimizzazione dei dati presenti nell'architettura del Prodotto.

I dati trattati mediante l'applicativo devono essere quelli strettamente indispensabili e necessari al perseguimento delle finalità cui il software è destinato, non essendo giustificabile trattare dati degli interessati che non siano pertinenti al raggiungimento degli scopi di trattamento.

Per **i Prodotti che pongono in essere trattamenti obbligatori per legge**, i campi sono quelli imposti per il raggiungimento della finalità imposto dalla legge stessa, quindi nelle attività di realizzazione del Prodotto il margine decisionale su quali dati trattare, che livello di dettaglio piuttosto che di aggregazione realizzare deriva in modo più o meno diretto dalle normative di settore, anche relative al settore di mercato dove i potenziali utilizzatori operano. Ogni trattamento di dati non esclusivamente funzionale al perseguimento della finalità normativa, in esubero pertanto, deve poter essere escluso nella attività di customizzazione, e ciò senza naturalmente pregiudicare il corretto funzionamento del Prodotto stesso.

Per i **Prodotti che invece pongono in essere trattamenti diversi da quelli obbligatori per legge**, vi è la discrezionalità rispetto alla tipologia di dati ed i conseguenti trattamenti da prevedere nell'architettura del software. Rispetto a tali applicativi è necessario *in primis* analizzare se i trattamenti effettuati sono disciplinati dalla normativa privacy. Si pensi ad esempio ad un CRM, oppure allo sviluppo di un'applicazione capace di geolocalizzare gli utenti, o, ancora, alla creazione di bussole biometriche: le peculiarità tecniche di ideazione per la realizzazione di tali prodotti devono tenere conto degli elementi più o meno direttamente desumibili dalla normativa privacy[3], la quale deve essere previamente analizzata, tradotta e traslata nel design del software. Considerato che le logiche di accountability investono anche l'Utilizzatore finale del Prodotto, e considerate altresì le differenti peculiarità rispetto all'Utilizzatore stesso, ad es. in base al settore di mercato, all'organizzazione, ai dati trattati dall'utilizzatore ecc., senza pregiudicare le funzionalità del Prodotto, l'architettura dovrebbe rendere possibili attività di settaggio quali ad esempio:

1. i campi di dati da includere/escludere dal trattamento;
2. il grado di aggregazione/disaggregazione dei campi;
3. la possibilità di pseudonimizzare in campi inclusi *(vedi infra)*;
4. la possibilità di cifrare i campi inclusi *(vedi infra)*;
5. la possibilità di impostare dei termini di retention ai campi inclusi *(vedi infra)*.

3.4 Elementi di Design obbligatori

Dalla normativa di settore, ci sono alcune funzionalità che l'applicato dovrebbe prevedere, in particolare:

[N.B. le sezioni contrassegnate con (*) potrebbero non essere pertinenti rispetto al Prodotto e/o alle modalità tecniche di funzionamento]

Trasparenza e tracciabilità dei consensi *(*)*	Tramite l'applicativo, l'Utilizzatore deve essere in grado di associare ai contatti degli interessati presenti nell'applicativo l'informativa privacy ad essi resa. Tramite l'applicativo, l'Utilizzatore deve essere in grado di dimostrare i consensi eventualmente resi dagli interessati presenti nell'applicativo, affinché siano dimostrabili.

[3] anche dai provvedimenti del Garante fino alla loro vigenza

Funzione di data retention	L'applicativo deve permettere all'Utilizzatore di decidere la possibilità che tutte o alcune tipologie di dati vengano cancellati e/o anonimizzati allo scadere dei termini che questo deciderà, preferibilmente in modo automatizzato. Per controllare il buon esito delle attività di cancellazione/anonimizzazione il Prodotto potrebbe effettuare automaticamente degli audit.
Loggatura degli amministratori di sistema *(*)*	L'applicativo deve permettere all'Utilizzatore di registrare in modo integro, incancellabile ed inalterabile il log in ed il log out degli amministratori di sistema.
Creazione di profili	L'Utilizzatore deve essere in grado di prevedere profilature di accesso differenziate dei soggetti autorizzati rispetto ai dati e alle funzionalità del Prodotto.
Cifratura	Il Prodotto deve permettere all'Utilizzatore di impostare se e quali dati cifrare. Tale misura deve essere particolarmente attenzionata laddove l'applicativo non tratti solo dati personali identificativi. Per controllare il buon esito delle attività di cifratura il Prodotto potrebbe effettuare automaticamente degli audit.
Pseudonimizzazione	Il Prodotto deve permettere all'Utilizzatore di impostare e in caso su quali dati procedure di pseudonimizzazione. Per controllare il buon esito delle attività di pseudonimizzazione il Prodotto potrebbe effettuare automaticamente degli audit.
Diritto di accesso dell'interessato	In caso di esercizio di istanza di accesso, il Prodotto deve essere in grado di poter reperire facilmente tutti i dati riferibili all'interessato, ivi ricomprendendo anche quelli elaborati dall'Utilizzatore. Per i servizi usufruiti dall'interessato via web l'esercizio del diritto potrebbe essere impostato anche mettendo a disposizione un'area dedicata.

Diritto di rettifica	In caso di richiesta di rettifica da parte dell'interessato il Prodotto deve poter prevedere di licenziare tale richiesta. Per i servizi usufruiti dall'interessato via web l'esercizio del diritto potrebbe essere impostato anche mettendo a disposizione un'area dedicata.
Diritto di cancellazione (c.d. oblio)	In caso di richiesta di cancellazione da parte dell'interessato il Prodotto deve poter prevedere di soddisfare tale richiesta. Per i servizi usufruiti dall'interessato via web l'esercizio del diritto potrebbe essere impostato anche mettendo a disposizione un'area dedicata.
Diritto di limitazione del trattamento *(*)*	In caso di richiesta di limitazione del trattamento da parte dell'interessato il Prodotto dovrebbe assicurare che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati, quindi il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato (c.d. contrassegno). La limitazione potrebbe essere assicurata: 1. traferendo temporaneamente i dati selezionati verso un altro sistema di trattamento, 2. rendendo i dati personali selezionati inaccessibili agli utenti. 3. rimuovendo temporaneamente i dati presenti applicativo.
Diritto di portabilità	In caso di richiesta di portabilità da parte dell'interessato i formati gestiti dal Prodotto devono permettere all'interessato medesimo di ricevere gratuitamente i dati in forma strutturata e leggibile informaticamente. La normativa non impone formati specifici, restando inteso che nelle fasi di sviluppo dovrebbero essere preferiti dei formati comunemente utilizzabili in un'ottica di interoperabilità (es. PDF). Per i servizi usufruiti dall'interessato via web l'esercizio del diritto potrebbe essere impostato anche mettendo a disposizione un'area dedicata.

3.5 Testing

Completato il design ed ultimato il Prodotto, è opportuno effettuare attività di test volti a valutarne la robustezza e la sicurezza, anche mediante penetration test.

Le attività di test devono essere condotte da soggetti competenti, anche interni, ma diversi da quelli che hanno fatto attività di sviluppo. In caso di problematiche ravvisate nelle attività di testing, è necessario decidere e successivamente implementare attività di remediation atte a risolvere le problematiche rilevate prima delle commercializzazione.

Tenuto conto delle peculiarità in ottica data protection eventualmente insite al Prodotto in ragione dei trattamenti effettuati (es. si pensi a software che trattano grosse moli di dati particolari) è opportuno stabilire una periodicità di rinnovo delle attività di testing, fermo restando quelle di Beta test in caso effettuate dall'Utilizzatore.

3.6 Prodotti su storage messi a disposizione dalla Società

Per i Prodotti che presuppongono anche attività di conservazione dei dati su sistemi messi a disposizione dalla Società, questa deve garantire:

[N.B. quanto di seguito indicato potrebbe non essere pertinenti rispetto al Prodotto e/o alle modalità tecniche di funzionamento e/o agli obblighi contrattuali in essere con l'Utilizzatore]

Attività	**Note**
di avere effettuato una valutazione del rischio informatico	Documentare lo status di rischio che deriva dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale ai dati conservati, trasmessi o comunque trattati
di aver posto in essere un piano di remediation per risolvere le problematiche di sicurezza rilevate	
di effettuare a seguito una nuova valutazione del rischio informatico, e comunque di effettuarla con le adeguate periodicità	
di avere un elenco delle misure di sicurezza fisiche a presidio dei dati ospitati	*N.B. in un'ottica di accountability potranno essere prese come spunto i contenuti delle ISO in materia di sicurezza informatica, nonché le best practices riconosciute a livello internazionale*.
di aver un elenco delle misure di sicurezza informatiche	di seguito si citano quelle desumibili dalla normativa • sistema di rilevazione dei data breaches; • backup dei dati; • loggatura ads

	• misure tecniche per assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi *N.B. in un'ottica di accountability potranno essere prese come spunto i contenuti delle ISO in materia di sicurezza informatica, nonché le best practices riconosciute a livello internazionale*.
di avere un elenco delle misure organizzative legate agli aspetti di sicurezza	di seguito si citano quelle obbligatorie ai sensi della normativa • procedura data breach; • procedure per ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico

3.7 *Subfornitori e terze parti*

Prima di acquisire ed implementare tali prodotti di terze parti, è pertanto necessario valutare se tecnicamente rispondono alle impostazioni di design che caratterizzeranno il Prodotto, anche sotto il profilo del rischio.

Se nell'architettura del Prodotto, oppure in riferimento a determinati aspetti di sicurezza, incidono anche specifiche tecnologiche che non dipendono in via diretta dalle scelte della Società, ma che derivano bensì da prodotti di terze parti, anche open source, gli aspetti fino ad ora considerati e comunque le decisioni che nella fase di ideazione sono state assunte, devono essere applicate anche a questi.

4. Revisione

Nell'ottica di assicurare la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali effettuato mediante gli applicativi, ai fini di garantire il rispetto degli aspetti di PbD nelle logiche dell'accountability del GDPR, la Società si riserva di aggiornare le presenti Linee Guida nei seguenti casi:

- modifiche normative o emanazione di best practices;
- variazioni organizzative e di business dell'azienda;
- upgrade tecnologici sia sotto il profilo delle funzionalità che dal punto di vista della sicurezza;
- dismissione degli applicativi;
- data breaches;
- reclami da parte degli Utilizzatori.