Comune di Fosdinovo

Provincia di Massa Carrara

REGISTRO DELL'ACCOUNTABILITY

PREMESSE

Il Regolamento UE 679/2016 prevede il fondamentale il principio dell'*accountability,* altrimenti detto della rendicontazione e responsabilizzazione.

Il Titolare del trattamento è tenuto ad adottare all'interno della propria struttura procedure, misure e ad assumere delle scelte che consentano di adeguarsi al nuovo Regolamento sulla Protezione dei Dati Personali delle Persone fisiche.

Il Titolare deve, infatti, essere in "grado di dimostrare" che il trattamento dei dati delle persone fisiche è effettuato conformemente al Regolamento UE.

Lo scopo del Registro di rendicontazione è quello di documentare le motivazioni poste a fondamento di ogni scelta e procedura adottate, nonché ogni accadimento che incida sulla privacy policy.

Si tratta, dunque, di un documento "*work in progress*" che richiede una gestione corretta ed aggiornata.

Il sistema di rendicontazione interno presuppone la necessità per il Titolare di ricevere flussi di informazione sulle misure tecniche ed organizzative, nonché sulle scelte interne che possano avere un impatto sulla *privacy by default* e sulla *privacy by design* (articolo 25 del Regolamento).

Per tale ragione, verranno sensibilizzati i dipendenti e verranno istituti dei Responsabili che dovranno fornire tempestive e corrette informazioni al Titolare del trattamento, tenuto alla rendicontazione interna.

Tale Registro sarà messo a disposizione del DPO (Data Protection Officer) e dell'Autorità Garante della Privacy durante i controlli e le verifiche ispettive.

DEFINIZIONI

Art. 4 Regolamento UE 2016/679 - Definizioni

Ai fini del presente regolamento si intende per:

1) «**dato personale**» (**C26-C27-C30**): "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".

Dalla definizione si comprende che i principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono ad una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi e tali da impedire o da non consentire più l'identificazione dell'interessato.

Interessante il dettato normativo "*qualsiasi informazione*" che lascia intendere come il legislatore faccia riferimento non soltanto ai dati identificativi, ma ad ogni tipo di informazione riguardante una persona fisica, ivi compresa la sua immagine o un codice di identificazione personale.

2) «**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".

Dalla definizione appare evidente che il Regolamento si applica a qualsiasi tipo di trattamento di dati, sia esso cartaceo che informatico/automatizzato.

3) «**limitazione di trattamento**» (**C67**): "il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro".

4) «**profilazione**» (**C24-C30-C71-C72)**: "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".

5) «**pseudonimizzazione**» (**C26-C28-C29**): "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";

6) «**archivio**» (**C15**): “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”.

Le figure del Regolamento

7) «**titolare del trattamento**» (**C74**): “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”.

La norma prevede che sia opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest’ultimo effettui direttamente o indirettamente, per il tramite di altri soggetti.

In particolare, il titolare del trattamento dovrebbe mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, così da dimostrare la conformità delle attività di trattamento al Regolamento UE n. 679/2016.

Tali misure dovrebbero tener conto della natura, dell’ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

8) «**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”.

9) «**destinatario**» (**C31**): “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”.

10) «**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”.

Azioni personali

11) «**consenso dell’interessato**» (C**32-33**): “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”. Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l’interessato

manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.

12) «**violazione dei dati personali**» (**C85**): "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";

13) «**dati genetici**» (**C34**): "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". È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, del DNA o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti.

14) «**dati biometrici**» (**C51**), che assieme ai dati genetici sono stati per la prima volta definiti col regolamento dal legislatore Europeo, ma che erano già stati introdotti dal Garante Privacy italiano. Per "dati biometrici" si intendono 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;

15) «**dati relativi alla salute**» (**C35**): 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. Nei dati in commento dovrebbero rientrare tutte le informazioni riguardanti lo stato di salute dell'interessato (ovvero la sua salute fisica o mentale passata, presente o futura).

Questi dati comprendono informazioni sulla persona fisica, quali ad esempio un numero, un simbolo o un elemento specifico attribuito a quella persona per identificarla in modo univoco ai fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici ed ogni altra informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte – sia esso un medico, un operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro -.

16) «**stabilimento principale**» (**C36-37**): a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in

cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «**rappresentante**» (**C80**): "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";

18) «**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";

19) «**gruppo imprenditoriale**» (**C37-C48**): "un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate";

20) «**norme vincolanti d'impresa**» (**C37-C110**): "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";

21) «**autorità di controllo**»: "l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51";

22) «**autorità di controllo interessata**» (**C124**): "un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo";

23) «**trattamento transfrontaliero**»: "a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b)trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro";

24) «**obiezione pertinente e motivata**»: "un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione";

25) «**servizio della società dell'informazione**»: "il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio".

26) «**organizzazione internazionale**»: "un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati".

PRINCIPI GENERALI RELATIVI AL TRATTAMENTO

Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Art. 5 Regolamento UE 2016/679 - Principi applicabili al trattamento di dati personali.

I dati personali sono (**C39**):

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione») (**C74**)".

Art. 6 Regolamento UE/2016/679 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti

condizioni: (**C40**)

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (**C42-C43**);

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (**C44**);

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (**C45**);

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (**C46)**;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (**C45 -C46)**;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (**C47-C50**).

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX (**C8-C10-C41-C45-C51**).

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita (**C8-C10-C41-C45-C51**):

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento. La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e) è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i

dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro (**C-50**):

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Art.7 - Condizioni per il consenso (C42, C43)

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Art.8 - Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (C38)

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 14 anni. Ove il minore abbia un'età inferiore ai 14 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

2. Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Art. 9 - Trattamento di categorie particolari di dati personali

1. È 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. (**C51**)

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi (**C51, C52**):

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (**C55, C56**);

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3 (**C53**);

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (**C54**);

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (**C53**)

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. (**C8, C10, C41, C45, C53**)

Art. 10 - Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Art. 11 - Trattamento che non richiede l'identificazione (C57, C64)

1. Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identifica

***

In ossequio al dettato normativo e, pertanto, in ottemperanza a detti principi, il Regolamento UE 679/2016 stabilisce la responsabilità generale del Titolare per qualsiasi trattamento di dati personali che quest'ultimo effettui direttamente o che altri effettuino per suo conto.

In particolare, il Titolare del trattamento è tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità al Regolamento, delle proprie attività di trattamento.

Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base ad una valutazione oggettiva, mediante la quale si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del Titolare del trattamento o del Responsabile del trattamento - in particolare per quanto riguarda l'individuazione del

rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, nonché l'individuazione di migliori prassi per attenuare il rischio - sono forniti, ad esempio, da codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni di un responsabile della protezione dei dati.

Il comitato (WP29) pubblica linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indica quali misure possono essere sufficienti, in tali casi, per far fronte al rischio.

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 UE 679/2016.

Al fine di poter dimostrare la conformità al Regolamento, il Titolare del trattamento deve adottare politiche interne e attuare misure che soddisfino, in particolare, i principi della protezione dei dati fin dalla progettazione (c.d. *'privacy by design'*) e della protezione dei dati di default (c.d. *'privacy by default'*).

Tali misure possono consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, nello pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare le caratteristiche di sicurezza.

CONFERIMENTO INCARICO DI *DATA PROTECTION OFFICER*

Il Comune di FOSDINOVO in persona del suo legale rappresentante *pro-tempore,* con sede in Via Roma n.4 (MS),

- in ottemperanza alle disposizioni regolamentari e alle relative linee guida emesse dall'Autorità il 13.12.2016, tradotte, emendate ed adottate in data 5.4.2017, nonché alla luce delle FAQ in merito pubblicate in aggiunta a quelle allegate alle linee guida suddette,

- in qualità di Titolare del trattamento, nel rispetto del principio di *accountability* che permea l'intero Regolamento UE 679/2016, ha conferito l'incarico all'avv. Marco Giuri, nato a Napoli (NA), il 27/05/1970, codice fiscale GRI MRC 70E27 F839K, così da ottemperare agli obblighi di legge (Allegato 1: *conferimento incarico*).

***

STATO ATTUALE DI CONFORMITÀ ALLA NORMATIVA VIGENTE

Il giorno 25/5/2018, data di prima verifica sull'organizzazione della struttura, è emersa una situazione di generale e sostanziale conformità alla normativa vigente.

ADEMPIMENTI COMPIUTI IN OTTEMPERANZA AL REGOLAMENTO UE 679/2016 (*Privacy by Design - Privacy by Default*)

Alla data del 25.5.2018, in esecuzione degli adempimenti imposti dal Regolamento UE 679/2016 e in ottemperanza ai principi in epigrafe richiamati, nell'ottica di implementare ed adeguare il sistema di liceità del trattamento dei dati, nel pieno rispetto del principio di accountability, il Titolare del trattamento ha proceduto ad apportare modifiche al proprio sistema informatico e alla sua struttura organizzativa, con l'obiettivo di porre in essere una *policy* di tutela preventiva dei dati personali e, dunque, impegnandosi fin dalla progettazione dei prodotti e dei servizi il cui utilizzo incida sulla sfera giuridica degli utenti finali.

L'adeguamento nei termini sopra descritti ha riguardato, in particolare:

A) INFORMATIVE E CONSENSI

B) PROCEDURE SUI DIRITTI DEGLI INTERESSATI

C) NOMINE INTERNE ED ESTERNE

D) NOMINA DPO

E) REGISTRI DEL TRATTAMENTO

F) MISURE DI SICUREZZA

G) FORMAZIONE E REGOLAMENTAZIONE INTERNA DI PRIVACY *POLICY* E SULL'USO DEGLI STRUMENTI DI LAVORO

H) REDAZIONE DPIA (*DATA PROTECTION IMPACT ASSESTMENT* O VALUTAZIONE D'IMPATTO)

I) PROCEDURA PER LA *PRIVACY BY DESIGN E BY DEFAULT*

L) PROCEDURA *DATA BREACH*

M) ADEMPIMENTI *PRO FUTURO*

Si procede con la rendicontazione delle scelte effettuate per l'adeguamento, al fine di illustrare lo "stato dell'arte", alla data di apertura del presente registro.

SUB A) INFORMATIVE E CONSENSI

In relazione ai principi richiamati, con particolare riferimento a quello di liceità del trattamento, è stata effettuata una mappatura dei trattamenti.

In ossequio ai principi sanciti nell'art. 5 del Regolamento UE 679/2016, si è proceduto alla redazione delle informative, prestando attenzione all'aspetto delle finalità e modalità del trattamento, delle comunicazioni all'esterno dei dati trattati, della liceità, adeguatezza e pertinenza, nonché della durata della conservazione dei dati.

Specificamente sono state redatte le seguenti informativi:

- ***Informativa per i cittadini e per tutti gli interessati***
- ***Informativa per i dipendenti***
- ***Informativa per il sito internet (privacy policy)***
- ***Informativa videosorveglianza***

- ***Informativa immagini***

SUB B) PROCEDURE SUI DIRITTI DEGLI INTERESSATI

Il Regolamento UE 679/2016 pone particolare attenzione ai diritti dell'interessato, elevati a diritti fondamentali dalla Carta di Nizza.

Il primo fra i criteri che sintetizza *l'accountability* è il principio di *privacy by design* e *privacy by default,* espresso dall'art. 25 del Regolamento e concretantesi nella necessità di configurare il trattamento, prevedendo - fin dall'inizio - le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo, ove il trattamento si colloca e dei relativi rischi.

In ottemperanza al dettato normativo europeo, con riferimento all'esercizio dei diritti da parte dell'interessato, il Titolare con il DPO ha previsto e messo a disposizione degli interessati una procedura per la gestione ed evasione delle richieste, nonché ha redatto e pubblicato sul sito internet del Comune di Fosdinovo prestampati standard, utilizzabili dagli interessati per l'esercizio dei loro diritti e per avanzare qualunque tipo di richiesta.

SUB C) NOMINE INTERNE ED ESTERNE

In ossequio ai principi richiamati, si è proceduto al rinnovo delle nomine a Responsabili del trattamento ed a Autorizzati al trattamento.

In particolare, si è previsto che ogni dipendente venga inquadrato quantomeno come autorizzato al trattamento, atteso che, in esecuzione delle prestazioni cui è preposto, questi entra (o può facilmente e/o occasionalmente entrare) in contatto con il dato personale, seppur a diverso livello (*allegato 2: nomine).*

Il Comune di FOSDINOVO ha, poi, provveduto all'individuazione e relativa nomina dei Responsabili esterni del trattamento *(allegato 3: nomine Responsabili esterni).*

SUB D) NOMINA DPO

Il Comune di Fosdinovo ha proceduto alla nomina del *Data Protection Officer* (come in epigrafe delineato) in ottemperanza al Regolamento UE 679/2016 ed alle Linee guida dettate in materia dall'Autorità Garante *(allegato 4: nomina DPO).*

In un'ottica di *accountability,* si evidenzia che la scelta del professionista, per l'assolvimento di questo delicato incarico, è ricaduta sull'avv. Marco Giuri, esperto in materia di tutela del trattamento dei dati personali e della relativa normativa, sia nazionale che europea.

SUB E) REGISTRI DEL TRATTAMENTO

In ottemperanza al dettato di cui all'art. 30 del Regolamento UE 679/2016, sono stati predisposti i registri delle attività di trattamento del dato, ove vengono descritti i processi di trattamento sistematico (ai sensi dei principi di *privacy by design* e *privacy by default*) e sono annotati anche gli eventi, ulteriori ed eventuali, che, non soltanto, hanno un potenziale lesivo o meramente modificativo, ma anche migliorativo del trattamento stesso.
Il Titolare, quale responsabile del registro, delega la tenuta e l'aggiornamento del registro delle attività di trattamento del Titolare, *ex* art. 30, comma 1, Reg. UE 679/2016, a: Donatella Serani (area Finanze), Marco Giorgi (Area Affari Generali) e Paolo Pavoni (Area Sviluppo e LL.PP.)

La tenuta e l'aggiornamento dei registri dei Responsabili, *ex* art. 30, comma 2, Reg. UE 679/2016, saranno affidate a ciascun Responsabile sopranominato, il quale porrà in essere tutti gli adempimenti del caso con la massima diligenza.
Il registro costruito è formato da unico *file Excel* composto da più fogli: precisamente un foglio corrispondente al Registro del Titolare e gli altri fogli corrispondenti ai registri dei Responsabili nominati.
Il file sarà tenuto su database conservato su server aziendale e accessibile ai Responsabili a ciò addetti. L'unicità del file darà modo al titolare di verificarne in ogni momento il contenuto e la sua tenuta.
Tale registro sarà revisionato e controllato a cadenza regolare.

Per quanto attiene ai Responsabili esterni, i registri dovranno da loro essere compilati, aggiornati, conservati ed esibiti nei termini di cui all'atto di nomina, conformemente all'art. 30 del Regolamento UE 679/2016.

SUB F) MISURE DI SICUREZZA

Il Comune di FOSDINOVO ha messo in atto le seguenti misure di sicurezza:

- sistemi di autenticazione mediante credenziali;

- sistemi di autorizzazione;

- sistemi di protezione della rete (firewall, antivirus, altro…..);

- salvataggio dei dati IN CLOUD;

- backup giornaliero, in cloud;

- sensibilizzazione e formazione di tutto il personale dipendente;

- limitazione degli accessi agli archivi al solo personale autorizzato;

- porte, armadi e contenitori dotati di serrature;

SUB G) FORMAZIONE E REGOLAMENTAZIONE INTERNA DI PRIVACY *POLICY* E SULL'USO DEGLI STRUMENTI DI LAVORO

Punto focale del principio di responsabilizzazione è la consapevolezza di quello che è il proprio operato, non solo da parte del titolare, ma anche dei responsabili e degli autorizzati.

La liceità del trattamento non può prescindere dalla conoscenza della norma regolamentare e delle più rilevanti Linee guida in materia, emanate dall'Autorità Garante.

In quest'ottica, il Titolare, in accordo con il DPO, ha svolto una formazione dapprima dei Responsabili privacy e poi di tutti i Responsabili di area relativa alla conoscenza della normativa e alla sua applicazione pratica.

Il corso è stato tenuto dall'avv. Marco Giuri, docente in materia di privacy alla Business School del Sole 24

Altro corso è stato tenuto dalla dott.ssa Nicoletta Giangrande, esperta in materia di privacy e collaboratrice del DPO

SUB H) REDAZIONE DPIA (DATA PROTECTION IMPACT ASSESTMENT O VALUTAZIONE D'IMPATTO)

In ossequio al dettato di cui all'art. 35 del Regolamento UE 679/2016, si è provveduto alla redazione della Valutazione d'impatto (o DPIA – Data Protection Impact Assesment).
Con tale procedura, in pieno recepimento del principio di accountability, si analizza il rischio di un determinato trattamento, focalizzando l'analisi sull'elemento del rischio e del potenziale impatto negativo che questo ha sui diritti e le libertà dell'interessato coinvolto.
Gli impatti sono analizzati calcolando i rischi di cui all'art. 32, comma 2, del Regolamento, dando conto delle contromisure adottate.
La DPIA è redatta dal Titolare, di concerto con il DPO ed in conformità alle prescrizioni del Regolamento (artt. 35 e 36, comprensivi dei Considerando 75-77), nonché alle relative Linee guida (allegato 6: DPIA).
In particolare, ricorrono le seguenti circostanze: trattamento su larga scala di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, o di dati relative a condanne penali e a reati di cui all'art.10, sorveglianza sistematica su larga scala di una zona accessibile al pubblico, uso di nuove tecnologie ex art. 35, co. 1, Regolamento 679/2016 (pubblicazione on-line dei dati).

SUB I) PROCEDURA PER LA *PRIVACY BY DESIGN* E *BY DEFAULT*

La nuova disciplina, relativa al trattamento dei dati personali, individua due momenti di particolare importanza nell'organizzazione e gestione dei dati personali: la progettazione e la continuazione del trattamento, ossia i c.d. principi di *privacy by design* e *privacy by default* (art. 25 del Regolamento UE 679/2016).
In particolare, il concetto di *privacy by design* è stato codificato per la prima volta nel 2010 (il termine è stato recepito dal sistema statunitense e canadese) e trattato nella 32ima Conferenza Mondiale dei Garanti della Privacy.

Con tale espressione - innovativa per il nostro ordinamento - si fa riferimento alla pianificazione *ex ante* di un qualsiasi progetto di trattamento (sia strutturale, sia concettuale), il quale, appunto, va pianificato già nella fase di primissima progettazione, nonché durante la sua esecuzione, fino alla sua ultima distribuzione, utilizzo e eliminazione finale (*privacy by design*).

Si assume inoltre che il trattamento rispetti i principi generali della protezione dei dati, quali la minimizzazione degli stessi e la limitazione delle finalità (*privacy by default*).

Il Titolare garantisce, dunque, che siano trattati, di *default*, solo i dati personali necessari per il conseguimento di una finalità specifica e che la quantità dei dati e la durata della loro conservazione non vadano oltre il minimo necessario per il perseguimento di dette finalità.

I principi richiamati sintetizzano nel miglior modo il principio di *accountability*, ossia la necessità di configurare il trattamento, prevedendo sin dall'inizio le garanzie indispensabili per soddisfare i requisiti del Regolamento e, per l'effetto, per tutelare i diritti degli interessati, tenuto conto del contesto complessivo ove il trattamento si colloca e dei relativi rischi.

La pianificazione del trattamento deve avvenire a monte, ovvero prima che il trattamento stesso abbia inizio (valutando, ad esempio, i mezzi di trattamento).

Tale valutazione richiede un'analisi preventiva e un impegno applicativo che parte dal titolare e che si sostanzia nell'esplicazione *in primis* della c.d. DPIA ossia "Valutazione d'impatto per la protezione dei dati".

Sub L) PROCEDURA *DATA BREACH*

In ossequio ai principi richiamati e agli articoli 33 e 34 del Regolamento UE 679/2016, si è elaborata una procedura di *Data Breach* ed un modello per le notificazioni al Garante, che rendano maggiormente gestibile l'eventuale situazione di crisi.

SUB M) ADEMPIMENTI *PRO FUTURO*

In ossequio al principio di '*privacy by design'*, come sopra descritto, sono stati previsti i seguenti adempimenti *pro futuro*:

-cambiamenti serrature porte/ modifica password/ acquisto di nuovi antivirus più aggiornati

***

Il "registro di *accountability*" è un documento dinamico (principio di *'privacy by design'*).

Per far si che il registro *de quo* sia una testimonianza dell'attività che il Titolare pone in essere per rendere lecito il trattamento del dato, è necessario annotare tutti gli accadimenti, siano essi ordinari che non ordinari, indicandone la *data di verifica,* la *tipologia* e *ogni particolare che a suo giudizio è rilevante*.

INDIVIDUAZIONE DEI DELEGATI ALLA TENUTA DEL REGISTRO

Il soggetto tenuto alla rendicontazione è il Titolare del trattamento.

Il Comune di FOSDINOVO delega alla rendicontazione e alla tenuta del registro ciascun Responsabile delegato, ciascuno per la parte di competenza.

REGISTRAZIONE EVENTI SUCCESSIVI AL 25/05/2018:

DATA	EVENTO	ESITO	NOTE