SCAF SOCIETÀ COOPERATIVA AUTOCUSTODI FIORENTINI ar.l.

PR.01 - Procedura
MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO PRIVACY

SOMMARIO

1 PARTE GENERALE

1.1 SCOPO

Il presente documento fornisce un indirizzo generale dettando indicazioni di principio per il corretto trattamento dei dati personali da parte di SCAF Società Cooperativa Autocustodi Fiorentini a r.l. ("SCAF"), alla luce del Regolamento (EU) 2016/679 sulla protezione dei dati. Tale disciplina, infatti, è diretta a garantire che il trattamento dei dati personali effettuato da SCAF si svolga nel rispetto dei diritti, delle libertà fondamentali nonché della dignità delle persone fisiche e giuridiche, con particolare riferimento alla riservatezza e al diritto alla protezione dei dati personali di tutti coloro che hanno rapporti con la Cooperativa.

1.2 CAMPO DI APPLICAZIONE

Il presente modello si applica a SCAF Società Cooperativa Autocustodi Fiorentini a r.l. ("SCAF") sia che ricopra funzioni di "Titolare del trattamento", che di "Responsabile del trattamento".
Per le definizioni di "Titolare" e di "Responsabile" ai fini del presente documento si prega riferirsi all'art. 4 del Regolamento (EU) 2016/679 sulla protezione dei dati.

1.3 DOCUMENTI DI RIFERIMENTO

- Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679
- D.lgs. 231/2001, "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica"

1.4 GLOSSARIO E ACRONIMI

GDPR: Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679 o solo "Regolamento";

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;

VIOLAZIONE DEI DATI PERSONALI: o “data breach”, è 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;

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;

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.

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;

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;

DPO:(Data ProtectionOfficer) o “Responsabile delle Protezione dei dati” ex art 37 GDPR

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;

DATI COMUNI: sono tutti i dati personali che non appartengono alle categorie dei dati particolari e giudiziari;

DATI GIUDIZIARI: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;

DATI PARTICOLARI: 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;

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;

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;

AUTORITÀ DI CONTROLLO: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

PROCESSO DECISIONALE AUTOMATIZZATO: decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;

GRUPPO IMPRENDITORIALE: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

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 GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

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;

2 PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

2.1 PRINCIPIO DI LICEITÀ

il trattamento dei dati personali è lecito solo se si basi sul consenso dell'interessato o, in alternativa,su un'altra base legittima prevista dal GDPR ex artt. 6 e 9.

3.1.1 IL CONSENSO

Quanto all'espressione del consenso vale la libertà della forma, purché sia espresso, ne deriva che può essere prestato anche per comportamento concludente.
Il consenso è valido se è:

a) libero:

senza condizionamenti o vincoli, e per essere tale, deve essere sempre revocabile[1]; inoltre, all'interessato va chiarito se ha meno l'obbligo di comunicare i dati e le conseguenze dell'eventuale mancata comunicazione[2] degli stessi;

b) specifico:

[1] Ex c.32 del GDPRin via esemplificativa costituisce espressione del consenso la selezione di una apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto.
La revocabilità del consenso è sancita all'art. 7 del GDPR.

[2] Ex art. 13.2 lett. E)

deve essere richiesto un consenso per ogni finalità;

c) informato:

deve essere preceduto da informativa ex artt. 13 e 14 GDPR;

d) inequivocabile;

deve esservi certezza sia rispetto al fatto che l'interessato l'abbia prestato, che rispetto al contenuto: il consenso può dunque essere tacito o presunto e deve essere manifestato attraverso una dichiarazione o azione positiva inequivocabile[3]. Nei moduli scritti la richiesta di consenso deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato[4]. La richiesta deve essere chiara, concisa, e non interferire immotivatamente con il servizio per il quale il consenso è espresso[5].

e) Esplicito,solo nei seguenti casi:

1. trattamento dei dati sensibili ex art. 9 GDPR;
2. trasferimento a Paese terzo o organizzazione internazionale ex art 44 e ss.GDPR;
3. decisioni basate su trattamenti automatizzati ex art. 22 GDPR;

Deve essere escluso in questi casi l'ammissibilità del comportamento concludente;non deve essere necessariamente documentato per iscritto né è richiesta la forma scritta che, tuttavia,rappresenta una modalità idonea a configurare l'inequivocabilità del consenso e il suo "essere esplicito":

il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

3.1.2 LE ALTRE CONDIZIONI DI LEGITTIMITÀ

In assenza di consenso, il trattamento deve considerarsi lecito se:

a) necessario nell'ambito di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso o ai fini della conclusione;
b) effettuato in conformità ad un obbligo di legge al quale il titolare è soggetto;
c) è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri;

[3] non sono ammissibili per esempio caselle pre-spuntate su un modulo

[4] ex art. 7.2 GDPR

[5] ex c. 32GDPR

d) se è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica e solo se nessuna altra condizione di liceità può trovare applicazione[6];

e) vi è un interesse legittimo del titolare o di terzi che prevale sui diritti e sulle libertà fondamentali dell'interessato[7];

Per i dati "particolari", ex c. 51 e ex art 9 del GDPR, si aggiungono ulteriori condizioni di legittimità, per cui il trattamento di tale categoria di dati è lecito, oltre che nelle ipotesi di cui sopra, se:

f) è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare in materia di diritto del lavoro, sicurezza sociale, protezione sociale, e se autorizzato dalla legge o dalla contrattazione collettiva nazionale in materia di lavoro e in presenza di garanzie adeguate per i diritti fondamentali e gli interessi dell'interessato;

g) è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona in caso di incapacità fisica nel prestare il consenso;

h) è effettuato nell'ambito delle 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[8];

i) riguarda dati personali resi manifestamente pubblici dall'interessato;

j) è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria[9];

k) è necessario per motivi di interesse pubblico rilevante sulla base del diritto nazionale o europeo[10];

l) è necessario ai fini della 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[11];

---

[6] es. se è essenziale ai fini umanitari, per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione, in casi di emergenze umanitarie, di catastrofi naturali o umane ecc.…

[7] es. se l'interessato è un cliente o è alle dipendenze del titolare, o trattare i dati per finalità di marketing diretto; trasmettere i dati all'interno del gruppo imprenditoriale ai fini amministrativi interni, compreso il trattamento dei dati personali dei clienti e dei dipendenti; trattare dati relativi al traffico in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione ecc...

[8] a condizione che il trattamento riguardi unicamente i membri o le persone che hanno regolari contatti con la fondazione, associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato.

[9] o ogni volta che le autorità giurisdizionali esercitino le loro funzioni giurisdizionali

[10] es. nei settori della sanità pubblica;

[11] conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al par. 3 del c. 53 del GDPR.

2.2 PRINCIPIO DI CORRETTEZZA

I dati devono essere trattati secondo lealtà e buona fede da osservarsi in tutte le fasi del trattamento comprese la fase preparatoria e la fase decisoria; gli interessati devono essere informati[12]circa la raccolta, l'utilizzo e la consultazione dei loro dati e sulle ulteriori tipologie di trattamento effettuate, precisando in che misura saranno effettuate al fine di garantire la trasparenza.

2.3 PRINCIPIO DI TRASPARENZA

Le informazioni[13]e le comunicazioni[14]relative al trattamento dei dati che il titolare deve fornire all'interessato, devono essere facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro; nel caso in cui l'interessato effettui una richiesta di esercizio dei diritti ex artt. 15-22 (dir. accesso, rettifica, cancellazione/oblio, portabilità, limitazione del trattamento) il riscontro, in virtù del principio in oggetto, deve essere dato, senza ritardo, al più tardi entro un mese, prorogabile fino a tre mesi con adeguata motivazione. L'esercizio di tali diritti deve essere gratuito per l'interessato, a garanzia del principio di trasparenza.

2.4 PRINCIPIO DI LIMITAZIONE DELLE FINALITÀ

I dati personali devono essere trattati per finalità determinate, esplicite e legittime, ossia per finalità lecite (cfr. **par. 3.1** del presente documento) e comunicate chiaramente all'interessato affinché sia in grado di conoscere le specifiche finalità, chiare ed univoche del trattamento dei suoi dati.
Il trattamento successivo dei dati raccolti deve essere compatibile, sulla base di una congrua valutazione ad opera del titolare, con le finalità originarie.
È tuttavia riconosciuto *ex lege* compatibile l'ulteriore trattamento per finalità di archiviazione nel pubblico interesse, per finalità statistiche, di ricerca scientifica e storica ovvero basato sul diritto nazionale o europeo e che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale.

[12]ex artt. 13 e 14 GDPR

[13] ex artt. 13 e 14 GDPR

[14]ex art. 12 GDPR

In caso di trattamento per finalità ulteriori, il titolare ha l'obbligo di informare l'interessato di tale altre finalità[15]**(*cfr. par. 5.1.1*)**e dei suoi diritti compreso il diritto di opporsi al trattamento ex art. 18 GDPR[16]**(*cfr. par. 5.6*).**

2.5 PRINCIPI DI MINIMIZZAZIONE DEI DATI

I dati personali trattati devono essere pertinenti, adeguati e limitati rispetto alle finalità - cd. "minimizzazione dei dati"; deve essere minimizzata la quantità dei dati raccolti quanto più possibile e limitarla ai dati strettamente necessari alle finalità predeterminate.
La minimizzazione si estende anche alla configurazione dei software e dei sistemi informativi, sin dalla fase della loro progettazione, utilizzati per trattare i dati personali[17]in modo da ridurre al minimo il loro uso*(cd. privacy by design*); nonché allo sviluppo di tecnologie e/o processi con l'obiettivo di raccogliere ed elaborare solo i dati personali strettamente necessari per consentire all'interessato di fruire della funzionalità richieste assicurando *by default* un trattamento legittimo (cd. *"privacy by default")*

2.6 PRINCIPIO DI ESATTEZZA

Il titolare deve assicurare l'accuratezza e la qualità delle informazioni personali, soprattutto quando il dato viene raccolto presso terzi, trattando dati esatti e aggiornati; in applicazione del principio in oggetto, l'interessato ha un diritto di rettifica e laddove i suoi dati sono inesatti o non aggiornati ha il diritto di ottenere, in via cautelativa, la limitazione del trattamento[18] per tutto il periodo necessario al titolare per le opportune verifiche e per effettuare, ove necessario, le procedure di rettifica; infine, se non sia concretamente possibile effettuarne l'aggiornamento o la rettifica dei dati, l'interessato ha il diritto di ottenere la cancellazione degli stessi. Il fatto che i dati siano esatti e aggiornati non rappresenta solo un diritto dell'interessato, ma specularmente, un vero e proprio dovere per il titolare, che deve rendere note le eventuali rettifiche operate sui dati all'interessato.

[15]ex art. 13.4 e 14.4 RGDP

[16]cfr. *"Procedura sull'esercizio dei diritti dell'interessato RE (UE) 2016/679"*

[17]cfr. opinioni 2/13 e 1/14 Gruppo di lavoro WP29

[18]ex art. 18 GDPR

2.7 PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

Di regola i dati devono essere conservati in una forma che permetta l'identificazione degli interessati per un lasso di tempo non superiore al conseguimento delle finalità onde evitarne un abuso contrario ai principi di correttezza, trasparenza e liceità[19].

2.8 PRINCIPIO DI INTEGRITÀ E RISERVATEZZA

Ai dati deve essere garantita una adeguata sicurezza; le informazioni devono essere salvaguardate nella loro esattezza (integrità) e difese da intrusioni e alterazioni non autorizzate (riservatezza). Il titolare deve adottare misure tecniche e organizzative affinché sia impedito l'accesso e l'utilizzo non autorizzato ai dati personali e alle attrezzature impiegate per il trattamento.

2.9 PRINCIPIO RESPONSABILIZZAZIONE

Si sostanzia nel rispetto dei principi suddetti e nella capacità del titolare di comprovarlo; il titolare è tenuto a mettere in atto misure adeguate ed efficaci per dimostrare, su richiesta dell'autorità di controllo, la conformità delle attività di trattamento al GDPR, compresa l'efficacia delle misure stesse.

3 SOGGETTI DEL TRATTAMENTO

3.1 SOGGETTI ATTIVI DEL TRATTAMENTO

4.1.1 IL TITOLARE DEL TRATTAMENTO

[19] Nel caso in cui i dati personali siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistica, sarà possibile conservarli, anche se permettono una re-identificazione dell'interessato, per periodi più lunghi rispetto al raggiungimento delle finalità, ma a condizione che si adottino le misure adeguate tecniche e organizzative richieste dal RGPR, volte a proteggere i diritti e le libertà dell'interessato.

Il titolare del trattamento può essere una persona fisica o giuridica, pubblica o privata, che determina le finalità e i mezzi del trattamento e il profilo della sicurezza dei dati personali.

Sotto il profilo della sicurezza:

a) Decide e mette in atto misure tecniche e organizzative adeguate di *by design* e *by default,* tra le quali quella, per cui, in caso di sviluppo di prodotti e/o sistemi basati sulle nuove tecnologie,impone contrattualmente allo sviluppatore di adottare già in fase di progettazione, misure di sicurezza e di minimizzazione dei dati fornirne evidenza documentale;

b) Procede alla valutazione di impatto e alla consultazione preventiva ex. art. 35 e 36 GDPR per le cui specifiche si rimanda al documento aziendale denominato "***Procedura per il data breach***";

c) Adotta le misure tecniche e/o organizzative adeguate di sicurezza valutandole periodicamente; si dota di policy interne e codici di condotta adeguati, linee guida e ulteriore documentazione aziendale, in materia di protezione dei dati;

d) Si conforma al principio di responsabilizzazione attenendosi al rispetto della correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, per l'intera durata del trattamento;

e) Individua ruoli subordinati all'interno della struttura (personale e/o collaboratori) cui affidare le operazioni di trattamento istruendoli adeguatamente e impartendogli istruzioni e direttive vincolanti;se esternalizza attività di trattamento deve obbligatoriamente designare gli outsourcer responsabili esterni del trattamento ex art. 28 GDPR e istruirli adeguatamente, autorizzandoli, se del caso, a designare a loro volta altri responsabili; svolge infine funzioni di controllo e vigilanza sul loro operato.

f) Designa nei casi previsti dalla legge e dal GDPR il DPO e lo supporta e coopera con lo stesso (cfr. **par. 4.1.3** del presente documento)

g) Predispone idonei strumenti di verifica del rispetto degli obblighi cui è soggetto il responsabile ex art. 28 GDPR;

h) In caso di violazione dei personali deve porre in essere misure idonee per porvi rimedio e, se del caso, per contenere la violazione dei dati o per attenuarne i possibili effetti negativi; deve, inoltre, procedere alla notificazione della violazione all'autorità di controllo competente e, ove necessario, comunicarla all'interessato; per le specifiche sul punto si rimanda al documento aziendale denominato ***"Procedura per il data breach";***

Profilo di garanzia dei diritti dell'interessato:

i) Il titolare adotta tutte le misure appropriate per fornire all'interessato le informazioni di cui all'art. 13, 14 e 13.4 e 14.4 GDPR; successivamente, si dota di idonea organizzazione per permettere l'esercizio esercizio dei diritti da parte degli interessati ex artt. 15-22 del GDPR; per le specifiche si rimanda al documento aziendale denominato ***"Procedura per l'esercizio dei diritti dell'interessato RE (UE) 679/16";***

Profilo della collaborazione con i soggetti preposti al controllo:

j) Coopera con l'autorità di controllo;
k) Coopera con gli organismi indipendenti di certificazione;
l) Coopera con il DPO;

4.1.2 I CONTITOLARI DEL TRATTAMENTO

Si tratta di due o più titolari che determinano congiuntamente le finalità e i mezzi del trattamento. Ciascuno dei contitolari è corresponsabile e tenuto al rispetto delle obbligazioni poste dal Regolamento Generale sulla protezione dei dati (EU) 2016/679, al fine di tutelare le persone fisica a cui i dati trattati si riferiscono.

Il riparto di responsabilità e ruoli assunti in merito alle obbligazioni imposte loro dal Regolamento; rispetto, per esempio al profilo della sicurezza del trattamento ex art. 32 GDPR, ovvero al profilo della collaborazione coi soggetti preposti al controllo ed in particolare, rispetto all'esercizio dei diritti degli interessati e alla comunicazione delle

informazioni ex artt. 13 e 14 GDPR, devono essere chiaramente definiti in un accordo ex art. 26 GDPR, i cui estremi devono essere resi noti agli interessati stessi già nella informativa nonché ulteriormente rese in sede di accesso ex art. 15 RGDP.

4.1.3 IL RESPONSABILE DEL TRATTAMENTO

È la persona fisica o giuridica, pubblica o privata, che tratta dati personali per conto del titolare del trattamento.
Deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.
È designato con contratto o altro atto giuridico, anche in forma elettronica, o dal titolare, o da altro responsabile dietro previa autorizzazione scritta del titolare specifica o generale. Il contratto,o altro atto giuridico, deve contenere le clausole minime inderogabili di cui all'art. 28.3. GDPR.

Il Responsabile deve procedere al trattamento secondo le istruzioni impartite per iscritto dal Titolare con contratto o altro atto giuridico che specifichi durata, natura e finalità del trattamento, tipo di dati personali, categorie di interessati, obblighi e diritti del Titolare.

- **Obblighi**

a) Il responsabile deve adottare misure per vincolare i propri incaricati (siano essi dipendenti o collaboratori) alla riservatezza;

b) In caso di autorizzazione generale, fornire informazione al titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili, affinché quest'ultimo possa, se del caso, opporsi;

c) Al termine della prestazione di servizi relativi al trattamento deve cancellare o restituire al titolare tutti i dati personali e cancellare le copie esistenti, salvo che il diritto dell'Unione la normativa nazionale preveda la conservazione dei dati;

d) Informare il titolare qualora ritenga che una istruzione da questi impartita violi il Regolamento o altre disposizioni nazionali o europee in materia;

e) Adottare misure tecniche e organizzative per garantire la sicurezza ex 32.1;

f) Assistere il titolare del trattamento al fine di soddisfare l'obbligo del titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;

m) Se necessario, e su richiesta, assistere il titolare del trattamento nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati e dalla previa consultazione dell'autorità di controllo;

g) Consentire e cooperare alle attività di revisione, comprese le ispezioni realizzate dal titolare del trattamento o da un altro soggetto da questi incaricato;

h) Cooperare su richiesta con l'autorità di controllo;

n) Designare nei casi previsti dalla legge e dal GDPR il DPO e supportarlo e cooperare con lo stesso (cfr. **par. 4.1.3** del presente documento);

o) Nei casi pervisti dalla legge ex art. 30 GDPR, tenere un registro delle attività di trattamento svolte per conto del titolare, in forma scritta, anche in formato elettronico, con obbligo di contenuto minimo indicato previsto ex art. 30.2. GDPR, il cui modello è allegato alla presente procedura;

4.1.4 IL RESPONSABILE PER LA PROTEZIONE DEI DATI

Il Responsabile della protezione dei dati, è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR[20]dal titolare del trattamento o dal responsabile del trattamento e deve:

[20] Dovranno designare obbligatoriamente un DPO: a) amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie; b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio

- possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati;
- adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse;
- svolgere i suoi compiti garantendo il segreto e la riservatezza;
- operare alle dipendenze del titolare o del responsabile oppure sulla base di un contratto di servizio (DPO esterno).

Il titolare o il responsabile del trattamento dovranno mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

- **Pubblicazione e comunicazione dei dati di contatto**

Una volta nominato, i dati di contatto del DPO, quali:

- Nome e cognome del RPD
- indirizzo di posta elettronica
- indirizzo di posta PEC
- indirizzo posta cartacea

devono essere tempestivamente:

a) comunicati via e-mail ai dipendenti e collaboratori;
b) pubblicati sul sito web della azienda e nella intranet aziendale;
c) comunicati alle autorità di controllo;

Inoltre, il contatto telefonico del DPO, dove essere inserito nell'elenco telefonico interno, e il ruolo ed il nominativo del DPO nell'organigramma aziendale.

regolare e sistematico degli interessati su larga scala; c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

Anche per i casi in cui il regolamento non impone in modo specifico la designazione di un DPO, è comunque possibile una nomina su base volontaria

- **Compiti del DPO**

Il DPO ha il compito di:

a) sorvegliare l'osservanza del GDPR, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;

b) collaborare con il titolare/responsabile, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);

c) informare e sensibilizzare il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;

d) cooperare con il Garante e fungere da punto di contatto per il Garante su ogni questione connessa al trattamento;

e) fungere da punto di contatto con l'interessato per l'esercizio dei diritti di cui agli art. 15-22 del GDPR;

f) supportare il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

- **Casi di consultazione preventiva obbligatoria del DPO**

È obbligatorio richiedere la consultazione preventiva al DPO:

a) In tutti i casi in cui debbano essere assunte decisioni che impattano sulla protezione dei dati personali; in tali casi il RPD è chiamato a rendere una consulenza idonea –tale parere deve essere tenuto in debita considerazione; è necessario documentare, in caso di disaccordo, le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal DPO;

b) In caso di violazione dei dati personali o altro incidente (cfr. procedura sulla data breach)

c) In caso di DPIA :

- Se condurre o meno il DPIA;
- Quale metodologia adottare nel condurre il DPIA;
- Se condurre il DPIA con le risorse interne ovvero esternalizzandola;
- Quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- Se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno col trattamento, e, quali salvaguardie applicare) siano conformi al GDPR;

In ipotesi di disaccordo con le indicazioni fornite da RPD, è necessario che la documentazione relativa al DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.

d) In ogni caso di sviluppo interno o esterno di prodotti e sistemi basati sulle nuove tecnologie, con comunicazione via e-mail anche alla Direzione Privacy, in ogni caso di sviluppo interno o esterno di prodotti e sistemi basati sulle nuove tecnologie, affinché l'ufficio del DPO possa prevalutare le misure di protezione dei dati e di sicurezza adottate dallo sviluppatore fin dalla progettazione/sviluppo.

4.1.5 RAPPRESENTANTE DEL TITOLARE E DEL RESPONSABILE

Se il titolare o il responsabile, non sono stabiliti nell'Unione Europea, ma trattano dati personali di interessati che si trovano nell'Unione e le attività di trattamento in questione sono connesse all'offerta di beni e servizi a tali interessati[21] devono obbligatoriamente nominare, con mandato scritto, un rappresentante, persona fisica o giuridica stabilita in uno dei paesi membri dell'Unione in cui si trovano gli interessati suddetti; la designazione non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento ai sensi della disciplina europea in materia di protezione dei dati contenuta nel regolamento.

Il rappresentante agisce per conto del titolare del trattamento o del responsabile del trattamento e

[21] Ad esclusione dei casi in cui: a) il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati personali o il trattamento di dati personali relativi alle condanne penali e ai reati, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento, b) se il titolare del trattamento è un'autorità pubblica o un organismo pubblico

può essere interpellato da qualsiasi autorità di controllo; funge, inoltre, da interlocutore in aggiunta o in sostituzione del titolare e/o del responsabile, degli interessati.

4.1.6 INCARICATI DEL TRATTAMENTO

Si tratta delle "persone autorizzate" al trattamento dei dati personali sotto la diretta autorità del titolare e/o del responsabile ex art. 4.10 RGDP.

3.2 SOGGETTI PASSIVI DEL TRATTAMENTO – GLI INTERESSATI

Sono le persone fisiche cui si riferiscono i dati personali oggetto del trattamento.

4 DIRITTI DEGLI INTERESSATI

4.1 DIRITTI CONOSCITIVI

5.1.1 DIRITTO ALL'INFORMATIVA

I. Nel caso in cui i dati sono raccolti direttamente presso l'interessato, l'informativa ex art 13 RGDP va data nel momento della raccolta dei dati personali e prima della stessa, con il seguente contenuto obbligatorio (**c.d. informativa diretta)**:

a) *Identità e dati di contatto* del titolare, degli eventuali contitolari e contenuto essenziale dell'accordo ex art 26 GDPR, dell'eventuale DPO;

b) *Finalità* del trattamento(es.: di marketing, di erogazione del servizio ecc.) del trattamento;

c) *Eventuali obblighi di legge o di contratto* alla base della fornitura dei dati personali e conseguenze del rifiuto;

d) *Base giuridica* del trattamento ex art. 6 RGDP (consenso, contratto, obbligo legale interesse pubblico ecc.…) e se è costituita dall' interesse legittimo del titolare o del terzo ai sensi dell'art. 6.1 lett. f) RGDP la specificazione dell'eventuale interesse legittimo;

e) *L' ambito di circolazione* dei dati con l'indicazione dei destinatari o delle categorie di destinatari ai quali i dati personali sono stati o possono essere comunicati (si tratta sempre dei responsabili esterni - oppure degli stessi incaricati, vale a dire i dipendenti dell'azienda)

f) L'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, o nei casi di cui all'art. 46 o 47 e 49.2 RGDP, il riferimento delle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;

g) *La durata del trattamento*, oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

h) *I diritti dell'interessato* di ottenere l'accesso ai dati ex art 15, la rettifica ex art. 16 GDPR o la cancellazione dei dati personali ex art. 17 GDPR, il diritto alla portabilità dei dati ex art. 20; o la limitazione del trattamento dei dati personali che lo riguardano ex art. 18 RGDP; e di opporsi al loro trattamento ex art. 21 RGDP;Il diritto a revocare il consenso ex art. 7 RGDP;di proporre reclamo all'autorità di controllo;

i) *L'eventuale esistenza di un processo decisionale automatizzato*, compresa la profilazione di cui all'art. 22.1 e 22.4, ed in tal caso, l'indicazione della logica applicata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

II. Quando i dati personali vengono raccolti da altro trattamento[22] del trattamento, l 'informativa va data entro un termine ragionevole e comunque non oltre un mese dall'ottenimento dei dati personali (**informativa successiva)**, salvo in caso in caso di comunicazione dei dati personali all'interessato o di rivelazione di essi a terzi, per cui è permesso procedervi al più

[22] Es. quando i dati sono raccolti da una fonte pubblicamente accessibile come una pagina web o pubblico registro.

tardi al momento rispettivamente della *prima comunicazione* o della *prima rivelazione*. Ai contenuti dell'informativa diretta vanno aggiunti:

j) l'origine dei dati personali (vale a dire, come ed eventualmente da quali fonti sono stati raccolti); in particolare, l'eventuale indicazione espressa che i dati provengono da fonti accessibili al pubblico;

k) le categorie di dati personali in questione (se comuni, speciali o giudiziari)

Non è necessario fornire *Eventuali obblighi di legge o di contratto* alla base della fornitura dei dati personali e conseguenze del rifiuto.

Non è dovuta ove:

- l'interessato dispone già delle informazioni;
- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato;
- previsione normativa espressa che permette la rilevazione dei dati o l'acquisizione degli stessi in un quadro di garanzie per l'interessato;
- tutela del segreto a cui è tenuto il titolare "successivo"

III. In caso di mutamento di finalità del trattamento rispetto a quelle per le quali erano stati raccolti precedentemente l'informativa (**ulteriore)**in ogni caso va data prima del trattamento per ulteriori finalità;oltre alle informazioni rese nella informativa diretta vanno aggiunte le seguenti informazioni supplementari:

l) indicazione della nuova finalità;

m) tempi di conservazione dei dati e, se non è possibile, i criteri utilizzati per determinare tale periodo;

n) *Eventuali obblighi di legge o di contratto* alla base della fornitura dei dati personali e conseguenze del rifiuto;

o) *L'eventuale esistenza di un processo decisionale automatizzato*, compresa la profilazione di cui all'art. 22.1 e 22.4, ed in tal caso, l'indicazione della logica applicata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

p) *I diritti dell'interessato* di ottenere l'accesso ai dati ex art 15, la rettifica ex art. 16 GDPR o la cancellazione dei dati personali ex art. 17 GDPR, il diritto alla portabilità dei dati ex art. 20; o la limitazione del trattamento dei dati personali che lo riguardano ex art. 18 RGDP; e di opporsi al loro trattamento ex art. 21 RGDP;Il diritto a revocare il consenso ex art. 7 RGDP;di proporre reclamo all'autorità di controllo;

se il titolare ha già fornito una informativa successiva in quanto non ha ottenuto i dati direttamente presso l'interessato, l'informativa ulteriore deve contenere le seguenti informazioni aggiuntive:

q) L'origine dei dati personali (vale a dire, come ed eventualmente da quali fonti sono stati raccolti); in particolare, l'eventuale indicazione espressa che i dati provengono da fonti accessibili al pubblico;

r) *Base giuridica* del trattamento ex art. 6 RGDP (consenso, contratto, obbligo legale interesse pubblico ecc.…) e se è costituita dall' interesse legittimo del titolare o del terzo ai sensi dell'art. 6.1 lett. f) RGDP la specificazione dell'eventuale interesse legittimo;

5.1.2 DIRITTO DI ACCESSO EX ART. 15 RGDP

L'interessato ha il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e se del caso, l'accesso e la comunicazione in forma intellegibile alle seguenti informazioni:

- *Estremi identificativi* del titolare, degli eventuali contitolari e contenuto essenziale dell'accordo ex art 26 GDPR, dell'eventuale DPO dei responsabili (i fornitori di servizi, cd. responsabili esterni: la lista è disponibile su richiesta presso il DPO);

- l'indicazione delle finalità del trattamento(es.: di marketing, di erogazione del servizio ecc.) del trattamento;

- l'indicazione dell'eventuale interesse legittimo del titolare o del terzo ai sensi dell'art. 6.1 lett. f) RGDP;

- L'indicazione della base giuridica del trattamento ex art. 6 RGDP (consenso, contratto, obbligo legale interesse pubblico ecc.…);

- le categorie di dati personali in questione (se comuni, speciali o giudiziari)

- l'indicazione dei destinatari o delle categorie di destinatari ai quali i dati personali sono stati o possono essere comunicati (si tratta sempre dei responsabili esterni - oppure degli stessi incaricati, vale a dire i dipendenti di SCAF)

- Se possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile i criteri utilizzati per determinare tale periodo;

- La esistenza del diritto dell'interessato di ottenere la rettifica ex art. 16 GDPR o la cancellazione dei dati personali ex art. 17 GDPR, il diritto alla portabilità dei dati ex art. 20; il diritto a revocare il consenso ex art. 7 GDPR o la limitazione del trattamento dei dati personali che lo riguardano ex art. 18 GDPR; e di opporsi al loro trattamento ex art. 21 GDPR;

- La esistenza del diritto dell'interessato di proporre reclamo all'autorità di controllo (Garante per la Protezione dei dati Personali)

- Se i dati non sono raccolti direttamente presso l'interessato, l'indicazione dell'origine dei dati personali (vale a dire, come ed eventualmente da quali fonti sono stati raccolti); in particolare, l'eventuale indicazione espressa che i dati provengono da fonti accessibili al pubblico;

- La conferma della esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22.1 e 22.4, ed in tal caso, l'indicazione della logica applicata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

- L'eventuale intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, o nei casi di cui all'art. 46 o 47 e 49.2 RGDP, il riferimento delle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili;

- Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie

- adeguate ex art. 46 RGDP relative al trasferimento (es. Model Contract Clauses, norme vincolanti d'impresa ecc.…)

4.2 DIRITTO DI RETTIFICA EX ART. 16 RGDP

L'interessato ha il diritto di richiedere:

a) la correzione/rettifica dei dati inesatti
b) la integrazione dei dati incompleti

La rettifica può riguardare solo dati oggettivi e non anche valutazioni che invece possono essere solo oggetto di richiesta di eventuali integrazioni (es. note o precisazioni).

La rettifica dei dati è specularmente un dovere del titolare che, deve comunicare all'interessato le modifiche effettuate dei suoi dati.

4.3 DIRITTO DI CANCELLAZIONE-OBLIO EX ART. 17 RGDP

Il diritto di cancellazione dei dati personali da parte dell'interessato può essere esercitato nei seguenti casi:

- Se i dati personali non sono più necessari rispetto alla finalità per cui sono stati raccolti e/o trattati;
- Se l'interessato revoca il consenso al trattamento dei dati ex art. 7 RGDP;

- Se l'interessato ha esercitato il diritto di opposizione ex art. 21 RGDP;
- Se i dati personali sono stati trattati illegittimamente;
- Se sussiste un obbligo di legge alla cancellazione dei dati;
- Se i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione al minore di anni 16;

Il diritto di cancellazione deve essere esteso anche a tutti gli altri titolari cui sono stati comunicati i dati e, in caso i dati sono stati diffusi/ resi pubblici[23] a tutti gli altri titolari che abbiano raccolto i dati per informarli di cancellare qualsiasi link ai dati stessi come anche di qualsiasi copia o riproduzione, tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare per adempiere a tale obbligo informativo.

La cancellazione dei dati deve avvenire in maniera definitiva da tutti i sistemi informativi aziendali; in alternativa alla distruzione dei dati si può procedere alla loro anonimizzazione purché effettuata con tecniche non ne consentano la re-identificazione.

4.4 DIRITTO DI LIMITAZIONE DI TRATTAMENTO EX ART. 18 RGDP

L'interessato ha il diritto di ottenere dal titolare la limitazione del trattamento dei dati che lo riguardano nei seguenti casi:

- in caso di violazione dei presupposti di liceità del trattamento dei propri dati personali;
- se chiede la rettifica dei dati ex art. 15 del RGDP nelle more di tale rettifica;
- nel caso in cui si oppone al trattamento dei propri dati personali ex art. 21 del RGDP;
- nel caso in cui i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o stragiudiziale;

La limitazione comporta, ad esclusione della conservazione, il divieto di qualsiasi tipo di trattamento del dato oggetto di richiesta salvo non ricorrano le seguenti circostanze:

- consenso dell'interessato
- accertamento dei diritti in sede giudiziaria
- tutela dei diritti di altra persona fisica o giuridica
- interesse pubblico rilevante

[23] per esempio pubblicati sul sito web dell'azienda

L'interessato deve essere preavvisato dal titolare della revoca del vincolo di limitazione del trattamento dei suoi dati personali.

Salvo che ciò non implichi uno sforzo proporzionato, il titolare deve tempestivamente informare della richiesta di limitazione e della cessazione di tale limitazione, tutti gli altri titolari cui sono stati comunicati i dati personali oggetto di richiesta ex art. 18 RGDP.

4.5 DIRITTO DI REVOCA DEL CONSENSO EX ART. 7 RGDP

L'interessato può richiedere in ogni momento senza motivazioni la revoca del consenso prestato al trattamento dei suoi dati personali (es. per profilazione o marketing diretto o informazione scientifica ecc.…).

Se il trattamento non è legittimato su altra base giuridica, a seguito della richiesta di revoca, i dati oggetto dell'esercizio del diritto devono essere cancellati o in alternativa anonimizzati ex art. 17.1 RGDP

Salvo che ciò non implichi uno sforzo proporzionato, il titolare deve tempestivamente informare della richiesta di revoca tutti gli altri titolari cui sono stati comunicati i dati personali oggetto di richiesta ex art. 7 RGDP.

4.6 DIRITTO DI OPPOSIZIONE AL TRATTAMENTO EX ART. 21 RGDP

L'interessato può esercitare il diritto di opposizione nei confronti dell'azienda/titolare solo:

- Se Il trattamento è necessario per soddisfare un interesse legittimo del titolare ex art 6.1 lett. f) RGDP inclusa la conseguente profilazione; L'opposizione deve essere motivata e il titolare può rifiutarla:
    a) Se esistono motivi legittimi cogenti e prevalenti sull'esercizio del diritto;
    b) In caso di esercizio del diritto in sede giudiziaria

- In caso di trattamento per finalità di marketing diretto inclusa la conseguente profilazione;

L'opposizione non deve essere motivata e non può essere rifiutata dal titolare;

- In caso di trattamento per finalità di ricerca scientifica o storica o per finalità statistica L'opposizione deve essere motivata e può essere rifiutata solo nel caso in cui il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

L'opposizione fa cessare in maniera definita e permanente il trattamento con la cancellazione o la anonimizzazione dei dati ex art. 17.1 GDPR.

4.7 DIRITTO DI PORTABILITÀ DEI DATI EX ART. 20 RGDP

L'interessato può richiedere la portabilità dei propri dati personali solo in caso di trattamenti automatizzati e solo se si tratta di:

- Dati trattati col consenso dell'interessato
- Dati trattati sulla base di un contratto stipulato con l'interessato
- Dati che sono forniti esclusivamente dall'interessato

L'interessato ha il diritto, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito al titolare, inoltre ha il diritto di chiedere che vengano trasmessi direttamente ad a un altro titolare del trattamento.

4.8 DECISIONI BASATE SU UN PROCESSO DECISIONALE AUTOMATIZZATO EX ART. 22 RGDP

L'interessato può richiedere ai sensi dell'art. 22 del RGDP di conoscere la logica applicata al trattamento e i dati personali che gli sono attribuiti in esito alla profilazione o al trattamento automatizzato e di ottenere, se del caso, l'intervento umano, e/o di esprimere la propria opinione e/o di contestarne la decisione a condizione che:

- La decisione produca effetti nella sfera giuridica dell'interessato;
- La decisione sia basata unicamente su un trattamento automatizzato compresa la profilazione

e, salvo che tale decisione:

a) sia necessaria per la conclusione o l'esecuzione del contratto con l'interessato;

b) sia prevista dalla legge;

c) si basi sul consenso dell'interessato.

5 TRASFERIMENTO DEI DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è vietato in linea di principio a meno che vi siano le specifiche garanzie che seguono:

a) adeguatezza del paese terzo riconosciuta tramite decisione della Commissione Europea;

b) in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia quali:

- clausole contrattuali tipo approvate dalla (cd. *standard model clause*) adottate dalla Commissione;
- norme vincolanti d'impresa (cd. BCR) approvate secondo la procedura ex art. 47 del GDPR;
- adesione a codici di condotta;
- adesione schemi di certificazione ex art. 46 GDPR
- clausole tipo di protezione dei dati adottate da una autorità di controllo;
- clausole contrattuali ad hoc autorizzate da una autorità di controllo;
- accordi amministrativi stipulati da autorità pubbliche autorizzati da una autorità di controllo;

c) in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni quali:

- consenso esplicito dell'interessato;
- se il trasferimento è necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- se il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

- se il trasferimento sia necessario per importanti motivi di interesse pubblico;
- se il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- se trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- se il trasferimento è effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.
- solo in via residuale, se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali.

6 SANZIONI

6.1 SANZIONI AMMINISTRATIVE PECUNIARIE

Ai sensi dell'art. 83 del GDPR, gli importi delle sanzioni amministrative pecuniarie per le imprese vengono calcolate in percentuale sul fatturatodell' impresa; sono previsti due livelli di importi massimi, il primo è, fino a 10.000,00 euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente se superiore; il secondo livello di sanzioni, invece va fino ad un massimo di 20.000,00 o, per le imprese, fino al 4% del fatturato mondiale annuo dell'esercizio precedente se superiore.

Ai sensi **dell'art. 83.4. lett. a)** GDPR gli obblighi, la cui violazione è soggetta alle **sanzioni pecuniarie di primo livello** sono i seguenti:

a) **art 8** – consenso per i minori da parte di coloro che esercitano la potestà genitoriale o di chi ne fa le veci;

b) **art. 11**- Trattamento che non richiede l'identificazione;

c) **art. 25**-Privacy by design e by default

d) **art. 26**-Accordo tra contitolari del trattamento

e) **art. 27**-Nomina dei rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione;

f) **art. 28**-Obblighi e compiti del responsabile del trattamento;

g) **art. 29** - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento;

h) **art. 30** - Tenuta dei registri delle attività di trattamento;

i) **art. 31**- Cooperazione con l'autorità di controllo;

l) **art. 32** – Adozione delle misure di sicurezza del trattamento;

m) **art.33**- Notifica data breach all'autorità di controllo

n) **art. 34** - Comunicazione del data breach all'interessato

o) **art. 35**- Valutazione d'impatto - DPIA

p) **art. 36** - Consultazione preventiva alla autorità di controllo;

q) **artt. 37 -38-39**– Designazione, posizione e compiti del responsabile della protezione dei dati;

Ai sensi **dell'art. 83.5.** GDPR gli obblighi, la cui violazione è soggetta alle **sanzioni pecuniarie di secondo livello** sono i seguenti:

a) **art. 5** – Violazione dei principi applicabili al trattamento di dati personali;

b) **art 6** - Violazione delle condizioni di liceità del trattamento;

c) **art. 7** - Violazione delle condizioni per il consenso e diritto di revoca;

d) **art. 9** – violazione delle condizioni di liceità per il trattamento di categorie particolari di dati;

d) **art. 10** – violazione delle condizioni di liceità per il trattamento dei dati personali relativi a condanne penali e reati;

e) **art. 13**– Violazione dell'obbligo di Informazione qualora i dati personali siano raccolti presso l'interessato;

f) **art. 14**- Violazione dell'obbligo di Informazione qualora i dati personali non siano raccolti presso l'interessato;

g) **artt.- 15-22**- Violazione dei diritti dell'interessato;

h) **artt. 44-49** – Violazione dei principi e delle condizioni per il trasferimento extra UE dei dati personali.

i) **83.5. lett d)** - Violazione di obblighi relativi a norme sulla protezione dei dati adottate a livello nazionale nell'ambito di: rapporti di lavoro, archivi storici, ricerca scientifica o storica o statistica, titolari soggetti a segreto professionale; chiese e associazioni religiose;

l) **83.5. lett e)** - Inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58.2, o il negato accesso in violazione dell'articolo 58.1 durante l'esercizio dei poteri d'indagine dell'autorità di controllo.

6.1 PARAMETRI PER L'APPLICAZIONE DELLE SANZIONI

le sanzioni pecuniarie sono inflitte in funzione delle circostanze di ogni singolo caso in cui ex art. 83.2 si tiene debito conto dei seguenti elementi:

a. la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b. il carattere doloso o colposo della violazione;
c. le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d. il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
e. eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f. il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g. le categorie di dati personali interessate dalla violazione;
h. la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i. qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del

trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j. l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k. eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

Se, in relazione allo stesso trattamento o a trattamenti collegati il titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

6.2 MISURE CORRETTIVE

Le sanzioni pecuniarie possono essere inflitte in aggiunta o in luogo di una seria misure correttive ex art. 58.2 che l'autorità di controllo può adottare;tra queste ce ne sono alcune particolarmente gravose quali:

a) ai sensi dell'art. 58.2 lett f) GDPR, l'autorità di controllo ha il potere di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

b) ai sensi dell'art. 58.2. lett g) l'autorità di controllo può ordinare la rettifica ex art. 16 GDPR, la cancellazione ex art.17 GDPR di dati personali o la limitazione del trattamento ex art.18 GDPR nonché la notificazione di tali misure ai destinatari cui sono stati trasmessi i dati personali ex artt. 19 e 17.2 GDPR

c) ai sensi dell'art. 58.2. lett j), l'autorità di controllo può ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.