Cooperativa Sociale Optimus
Gestione Comunità per Minori
Via Cebrosa 86 10156 Torino (To)
Cell. +39 347 7154083 direzione@cooperativasocialeoptimus.it

Regolamento Europeo 679/2016 sulla Data Protection – (GDPR)

Applicata alle Unita' d'Offerta gestite dalla Cooperativa Sociale Optimus

Aggiornamento Privacy 04 Dicembre 2021

Premessa

Entrando a far parte dell'Unione Europea, lo Stato italiano ha rinunciato ad una parte della propria sovranità cedendola all'UE.
Il sistema delle fonti di diritto interno, di conseguenza, si è adeguato a tale situazione istituzionale, riconoscendo agli atti legislativi europei un valore differente a seconda della loro tipologia. I Regolamenti europei hanno la caratteristica di essere direttamente applicabili e obbligatori in tutti i loro elementi nei confronti di tutti gli Stati membri e di tutti i cittadini dell'Unione. Si collocano quindi, nel sistema di fonti normative interne, immediatamente al di sotto della carta costituzionale, prevalendo sia sul diritto interno già vigente che su quello successivo.
In base al dettato dell'art. 99 del GDPR, il Regolamento Europeo 679/2016 sulla Data Protection (GDPR) si applicherà **a decorrere dal 25 maggio 2018** e sarà obbligatorio in_tutti i suoi elementi nonché direttamente applicabile in ciascuno degli Stati membri. Dalla stessa data sarà abrogata la Direttiva 95/46/CE che attualmente disciplina a livello comunitario il trattamento dei dati.
Sempre in ambito di data protection, è attualmente vigente nel nostro Paese il Codice della Privacy (D.lgs 196/2003) con cui il legislatore italiano ha voluto raccogliere in un testo unico la maggior parte delle disposizioni inerenti alla privacy e al trattamento dei dati, recependo in tal modo la direttiva di cui sopra e quella sull'e-privacy (dir. 58/2002/CE).
Nonostante il Regolamento prevalga sulla legge nazionale interna, tuttavia la sola esistenza ed applicazione del GDPR **non comporta**, provenendo questo da un ordinamento (quello europeo) diverso da quello nazionale, **l'abrogazione automatica della legge statale regolante la medesima materia.**
Sebbene formalmente ancora vigenti, tutte quelle disposizioni della legge interna in contrasto con le nuove previsioni normative europee dovranno essere in ogni caso disapplicate, in favore della nuova disciplina. Il D.lgs. 196/2003 non subisce dunque alcuna abrogazione diretta e, al contrario, mantiene la sua forza normativa, subendo tuttavia una sorta di **"rilettura in chiave GDPR".** In base a tale "rilettura":
a) Dove non vi è compatibilità tra quanto disposto dal Codice della Privacy e quanto previsto dal Regolamento 679/2016, il CdP lascia il passo alle nuove disposizioni europee: la legge statale deve essere disapplicata in favore del GDPR;
b) Laddove vi sia compatibilità tra le due norme, il d.lgs. 196/2003 rimane applicabile continuando a dettare legge, anche in maniera più specifica rispetto al GDPR.

Il Regolamento europeo non parla di misure minime, ma si esprime solamente in **termini di adeguatezza**: l'art. 32 GDPR recita infatti che *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".
Nonostante sia presente un elenco esemplificativo e non esaustivo di misure tecniche e organizzative di sicurezza, il Regolamento non effettua una tipizzazione puntuale come quella dell'allegato B del CdP: tale scelta è in linea con il *principio dell'accountability* su cui si basa l'intero GDPR.

Titolare e responsabile del trattamento devono responsabilizzarsi e mettere in atto misure di sicurezza adeguate alla loro realtà aziendale.

COSA CAMBIA

Le principali novità contenute nel regolamento Europeo Privacy riguardano la diffusione dei dati personali e diritto all'oblio. Il nuovo testo, infatti, introduce il "diritto all'oblio" , regolamentato dall'art. 17 GDPR : "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione"

Il Regolamento Europeo Privacy introduce inoltre l'art. 5 che prevede una serie di principi nell'ambito del trattamento dei dati come quello della "*RESPONSABILIZZAZIONE*" che attribuisce direttamente ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare tutti gli altri principi pertanto le aziende dovranno dotarsi oltre che di un Responsabile della protezione dei dati (Data Protection Officer –DPO-) anche di un Registro delle Attività di trattamento e prepararsi alla notifica delle violazioni dei dati che andranno nell'arco di 72 ore comunicate al

Garante.

Diritto all'oblio

La Cooperativa Sociale Optimus si impegna a garantire all'interessato il diritto di ottenere senza «indebito ritardo» la **cancellazione dei dati personali** che lo riguardano, qualora si presentino le seguenti condizioni:

- i dati non sono più necessari in rapporto agli scopi per i quali sono stati ceduti o trattati;
- l'interessato ritira il consenso su cui si fonda il trattamento e non sussiste altro motivo legittimo per trattare i dati;
- l'interessato si oppone al trattamento dei dati personali;

- i dati sono stati trattati in maniera illegittima o devono essere cancellati in conformità a una legge dell'UE o di uno Stato membro, alla quale è soggetto il titolare del trattamento.

Cosa proteggiamo : Tipologie di dati

DATO PERSONALE	DATI PARTICOLARI
Qualunque informazione relativa a persona fisica che renda questa identificata e/o identificabile (anche indirizzo e-mail, numero civico etc.)	Dati sensibili che rilevano l'origine razziale,etnia, opinioni politiche e religiose, dati genetici, sanitari, orientamento sessuale
DATI GIUDIZIARI	**DATO ANONIMO**
Dati personali relativi alle condanne penali e ai reati nonché alle condanne connesse	Il dato che in origine o a seguito di trattamento non può essere associato ad un interessato identificato o identificabile

Definizione di trattamento

La Cooperativa Sociale Optimus attiva la procedura del trattamento per: qualunque operazione o insieme di operazioni, svolte con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, (raccolta, registrazione, organizzazione, strutturazione, conservazione, etc.)

Principi da adottare

La Cooperativa Sociale Optimus intende adottare i seguenti principi nello svolgimento del trattamento dei dati:

Liceità, correttezza e trasparenza	Il trattamento dei dati deve avvenire in modo lecito e corretto, informando i soggetti interessati circa la raccolta, l'utilizzo, la consultazione e la diffusione a terzi
Limitazione della finalita'	I dati raccolti devono essere pertinenti e adeguati rispetto alle finalità, raccogliere solo quelli che effettivamente sono funzionali al perseguimento delle finalità
Minimizzazione dei dati raccolti	Limitare la raccolta minimizzando la quantità di dati acquisiti ai soli dati necessari per il perseguimento delle finalità
Limitazione della conservazione	I dati raccolti devono essere conservati solo per il tempo necessario al perseguimento delle finalità per le quali sono stati acquisiti
Sicurezza dei dati	Gestione del rischio di perdita dei dati raccolti Data Breach

I **DOCUMENTI**

L'informativa

La Cooperativa Sociale Optimus si impegna a sottoporre a tutti gli interessati del trattamento **PRIMA dell'acquisizione dei dati**, l'Informativa che espone in modo semplice e chiaro le modalità con i quali i dati saranno trattati, il fine per i quali sono richiesti, il tempo nel quale saranno trattati e i diritti dell'interessato.

Per informativa si intende quell'insieme di informazioni che
il titolare del trattamento è tenuto a fornire ad ogni interessato, verbalmente o per iscritto.
L'informativa fornisce al soggetto interessato informazioni fondamentali, come:

(1) Quali sono gli scopi i tempi e le modalità del trattamento;
(2) Se l'interessato è obbligato o no a fornire i dati;
(3) Quali sono le conseguenze se i dati non vengono forniti;
(4) A chi possono essere comunicati o diffusi i dati;
(5) Quali sono i diritti riconosciuti all'interessato;
(6) Chi sono il titolare e l'eventuale responsabile del trattamento;
(7) Dove sono raggiungibili questi soggetti.

Il Consenso Informato

Per consenso si intende "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" (art. 4 punto 11). Il Garante pone in capo al titolare del trattamento l'onere di essere in grado di dimostrare che l'interessato ha effettivamente prestato il proprio consenso in maniera conforme a quanto previsto dal GDPR. La richiesta di tale consenso deve essere comprensibile, facilmente accessibile, il consenso può dirsi davvero informato quando le informazioni destinate agli interessati sono concise, facilmente accessibili e di facile comprensione e quando è utilizzato un linguaggio semplice e chiaro. L''interessato deve essere informato del diritto a revocare il proprio consenso in qualsiasi momento con la stessa facilità con cui è stato accordato. La revoca del consenso non retroagisce e dunque il trattamento compiuto prima della stessa rimane lecito.

Il Registro dei trattamenti

Secondo il GDPR Titolari e Responsabili del Trattamento, e nel caso i loro Rappresentanti, ciascuno per la propria parte, hanno l'obbligo di compilare in forma scritta, anche elettronica, il Registro delle attività di trattamento svolte dall'organizzazione. **È prevista una deroga per le organizzazioni con meno di 250 dipendenti**, se:

- le attività di trattamento effettuate non presentano un rischio per i diritti e le libertà dell'interessato;
- il trattamento è occasionale o non include particolari categorie di dati (tutti quelli atti a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose
- filosofiche, l'appartenenza sindacale, ovvero informazioni relative alla salute o alla vita sessuale o all'orientamento sessuale della persona) e non includa dati genetici o biometrici;

- il trattamento è occasionale o non include dati personali relativi a condanne penali e a reati.

Il Registro contiene una serie di informazioni che differiscono leggermente tra di loro a seconda che il compilatore sia il Titolare o il Responsabile. Esso, su richiesta, deve essere messo a disposizione dell'Autorità Garante.
Costruire il Registro dei Trattamenti significa comporre una mappa che contiene tutte le informazioni in merito a:

- le operazioni che l'organizzazione effettua sui dati personali;
- le caratteristiche dei dati personali oggetto di trattamento;
- le entità coinvolte nel trattamento dei dati personali.

Molte organizzazioni non sono consapevoli della quantità di informazioni personali di cui sono in possesso e, spesso, non sanno neanche con certezza dove e a quale scopo siano conservate.
Per questo, decidere di dedicare del tempo a reperire le informazioni e a metterle ordinatamente su carta o su un foglio elettronico permetterà di:

- avere una chiara rappresentazione di come i dati personali sono elaborati, protetti, archiviati ed eliminati;
- disporre di un patrimonio sempre aggiornato di conoscenza condivisa;
- intervenire in modo mirato soltanto dove ce ne sia un effettivo bisogno;

apportare migliorie ai processi, ottimizzando tempo e risorse

Considerato lo stato dell'arte e le risorse umane ed economiche

Considerate le indicazioni della normativa che ne prevede l'adozione per le società con più di 250 dipendenti

Considerato che la Cooperativa Sociale Optimus non tratta dati in larga scala

Considerato che il trattamento dei dati non è la principale attività della Cooperativa

Considerato che trattiamo dati di 30 utenti residenti e che pertanto non vi è una costante acquisizione di dati

La Cooperativa Sociale Optimus, al momento, non ha adottato il registro dei trattamenti, ma con la nomina del DPO si riserva di integrare tale strumento.

Le figure del GDPR

Il Titolare del Trattamento dei Dati

Il Titolare del trattamento (data controller) è colui che "da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali " (direttiva 95/46, art. 2 lett. d), e decide quali categorie di dati personali devono essere registrate (Convenzione 08, art. 2 lett. d). O anche, è *"la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza"* (Codice in materia di protezione dei dati personali, art. 4). In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati.

L'introduzione del nuovo regolamento generale europeo ha creato qualche problema nella traduzione dei termini, in quanto il termine ***data controller*** va tradotto, come stabilito dal Garante italiano, con titolare del trattamento, cioè colui il quale è responsabile per il trattamento medesimo. Questo ha creato qualche confusione col responsabile del trattamento, che invece più correttamente è la traduzione di ***data processor***.

Il titolare del trattamento non è, quindi, chi gestisce i dati, ma **chi decide il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa,** sia nazionale che internazionale, in materia di protezione dei dati personali, compreso l'obbligo di notifica al Garante nei casi previsti. Tra questi obblighi è importante ricordare che il titolare del trattamento deve porre in essere misure tecniche e organizzative adeguate per garantire, sin dalla fase della progettazione, la tutela dei diritti dell'interessato (Privacy by desygn). Il titolare è sempre vincolato al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento. Quindi egli deve garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente. In tale prospettiva spetta a lui stabilire le misure adeguate di sicurezza.

Qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, il titolare **è l'ente nel suo complesso** (ad esempio, la società, il ministero, l'ente pubblico, l'associazione, ecc .

Responsabilità
Nel caso di trattamento in violazione delle norme del regolamento europeo, il titolare risponde per il danno cagionato all'interessato, secondo quanto previsto dall'articolo 82 e dal Considerando 146. Il titolare risponde in caso di violazione delle disposizioni del GDPR, ma anche delle norme attuative, degli atti delegati, delle norme esecutive e di tutte le altre disposizione degli Stati membri.
Se più titolari o responsabili sono coinvolti nello stesso trattamento e sono responsabili del danno causato, ne rispondono in solido per l'intero danno, al fine di garantire l'intero risarcimento. Ovviamente chi paga l'intera somma avrà diritto di regresso nei confronti degli altri responsabili per la quota. Il titolare e il responsabile saranno esonerati da responsabilità se dimostrano che l'evento dannoso non è imputabile alla loro condotta, o se dimostrano di aver adottato tutte le misure idonee per evitare il danno stesso.

Il Responsabile del Trattamento dei Dati

Il titolare nomina con contratto o atto giuridicamente valido, il responsabile del trattamento, insieme al quale pone in atto le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio. Come nel caso del titolare del trattamento, anche la figura del responsabile del trattamento, sotto il profilo delle sue caratteristiche soggettive e delle sue responsabilità, è definito dal GDPR negli stessi termini già previsti dalla Direttiva 95/46/CE e dal Codice
Privacy. Nello specifico con tale nomina il GDPR si riferisce a : *"persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento"* (art. 4, paragrafo 1, n. 8). Si tratta quindi di quel soggetto che è preposto e al quale viene affidato, da parte del titolare, il trattamento dei dati personali dovrà avere pertanto una **conoscenza specialistica** della materia (comprovata eventualmente anche da attestazioni di frequenza di corsi), **affidabilità** e possesso di **risorse** che permettano di attuare misure tecniche e organizzative in grado di soddisfare tutti i requisiti stabiliti dal Regolamento per il trattamento dei dati personali, anche sotto il profilo della sicurezza.

Il Responsabile della Protezione dei Dati (DPO)

Per rendere la protezione dei dati ancora più sicura ed effettiva il Regolamento (UE) 2016/679 ha previsto la figura del Data Protection Officer (DPO) ovvero il responsabile della sicurezza dei dati. Il DPO è un professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati. Viene designato sistematicamente dal titolare e dal responsabile del trattamento in tre occasioni:
1.quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico (ad eccetto delle autorità giurisdizionali nell'esercizio delle loro funzioni); 2.quando i trattamenti consistono e richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
3.quando il trattamento riguarda, su larga scala, dati sensibili o relativi a condanne e reati.

In tutti gli altri casi è facoltà dei titolari e responsabili del trattamento, nonché di loro associazioni o altri organismi che li rappresentano, designare il responsabile della protezione dati che può agire per dette associazioni e organismi. Il DPO viene selezionato e scelto in base alle sue qualità professionali e in particolar modo il titolare e il responsabile del trattamento devono considerare la preparazione del DPO in ambito di trattamento dati, sia sul piano teorico che su quello pratico. Tale figura può essere selezionata tra i dipendenti del titolare del trattamento oppure può essere un libero professionista, esterno e autonomo, ingaggiato in base a un contratto di servizi. In ogni caso, i dati di contatto del DPO devono essere pubblicati e resi noti agli interessati oltre ad essere comunicati all'autorità di controllo competente. Il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti la protezione dei dati nonché sostenuto nell'esecuzione dei suoi compiti dal titolare e dal responsabile del trattamento che gli devono fornire tutte le risorse necessarie sia per svolgere il suo lavoro, sia per permettergli di mantenere aggiornata la sua conoscenza specialistica. In qualunque caso il lavoro del DPO deve svolgersi in assoluta

autonomia e indipendenza: nessuno può dargli alcuna istruzione circa l'esecuzione dei suoi compiti e il responsabile della protezione dati non può svolgere altre mansioni o compiti in conflitto di interessi con quelle proprie del DPO, essendo tenuto in ogni caso al segreto e alla riservatezza in ordine alle sue funzioni di responsabile della protezione. L'articolo 39 del Regolamento specifica poi nel dettaglio quali sono i compiti minimi del DPO:

- informare e fornire consulenza al titolare e al responsabile del trattamento in merito agli obblighi derivanti dal Regolamento 679/2016 o dalle altre disposizioni legislative.
- sorvegliare l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento in tutte le sue parti, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento;
- fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo fungendo, tra le altre cose, da punto di contatto per questioni connesse al trattamento effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

Infine è un diritto degli interessati contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati. L'introduzione di tale figura serva non solo a spostare da un soggetto (titolare e responsabile del trattamento) ad un altro (il DPO appunto) tutta una serie di responsabilità in ambito di protezione dei dati, ma anche e soprattutto per permettere ad un soggetto specifico, specializzato, esperto in materia di occuparsi esclusivamente della protezione dei dati personali, rimanendo sempre aggiornato sui rischi, i problemi e le misure di sicurezza necessarie a garantire un livello di tutela adeguato. Il tutto in linea con l'importanza, la diffusione e la complessità che l'ambito della privacy e del trattamento dei dati (soprattutto in campo digitale e tramite web) sta sempre più acquisendo.

Le imprese devono quindi, se vogliono garantire standard di sicurezza adeguati, nominare tali figure anche laddove ciò non sia obbligatorio per legge, possibilmente affidando tale compito a soggetti terzi ed esterni: il DPO, infatti, riferisce direttamente ai vertici aziendali e non al titolare/responsabile del trattamento (sebbene anche questi ultimi siano suoi superiori).

Incaricati del trattamento

Anche se nella traduzione italiana del GDPR non compare mai il termine incaricato del trattamento e pur non essendo espressamente prevista dal GDPR questa figura come figura giuridicamente autonoma, il Garante italiano, nella guida all'applicazione del Regolamento, giustifica e considera non incompatibile con il regolamento la figura dell'incaricato. Infatti, nel documento del Garante "**Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali** ", voce dell'indice "TITOLARE, RESPONSABILE, INCARICATO DEL TRATTAMENTO", sezione "Cosa non cambia?" si trova scritto

[*Pur non prevedendo espressamente la* ***figura dell' "incaricato" del trattamento*** *(ex art. 30 Codice), il regolamento* ***non ne esclude*** *la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento).*] [6]

Quindi anche se il GDPR non prevede la figura autonoma dell'incaricato, questo non vieta che se il titolare o il responsabile del trattamento, oltre a fare tutto quello che il regolamento espressamente prevede per "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile", vogliono anche fare (su base volontaria) una ulteriore responsabilizzazione di queste persone attraverso una specifica lettera di attribuzione di incarico e identificare queste persone utilizzando il termine "Incaricato" lo possono fare. Questa modalità operativa potrebbe anche essere considerata una buona prassi volta a poter ulteriormente sostenere la dimostrabilità della compliance al GDPR. Ma questa facoltà non deve essere intesa come un obbligo normativo come lo è invece per il Codice Privacy la nomina a incaricato prevista dall' art. 30, che al punto 2 prevede che la designazione dell'incaricato sia effettuata per iscritto e che nell'atto di nomina si debba individuare puntualmente l'ambito del trattamento consentito.
Se poi in fase ispettiva da parte della DPA venissero trovate prove documentali che comprovassero la perfetta e formale attribuzione delle nomine a incaricati di tutti i dipendenti alla stessa dovrà essere anche dimostrato che a **TUTTI I DIPENDENTI INCARICATI siano state impartite tutte le istruzioni da parte del titolare ed una adeguata formazione.** La Cooperativa ha provveduto a distinguere due categorie di incaricati al trattamento dei dati personali: incaricati interni, all'interno della quale vi fanno parte gli operatori in forza all'interno della Cooperativa e incaricati esterni, ossia tutte le figure professionali che entrano in contatto con i dati personali degli ospiti e degli operatori ai fini fiscali, amministrativi e ai fini sanitari.

ORGANIGRAMMA DELLA PRIVACY PRESSO LA COOPERATIVA SOCIALE OPTIMUS

Descrizione dell'attivita' svolta

La Cooperativa Sociale Optimus, opera nel comprensorio dell'ATS di Monza Brianza e Insubria, offrendo i propri servizi a tutto il territorio Lombardo e non. La Cooperativa Sociale Optimus accoglie minori in Comunita', offrendo loro interventi educativi e pedagogici finalizzati a salvaguardare il loro benessere psico-fisico, le capacita' relazionali, i percorsi
educativi e la loro salute mentale.
Le Comunita' si fanno carico di minori provenienti da famiglie problematiche e di minori migranti, inviati dai Servizi Sociali e Sanitari, dai Tribunali Minorili, e dai Responsabili della Giustizia Minorile.
Le Comunità della Cooperativa Sociale Optimus si presentano come strutture a carattere residenziale organizzate per accogliere utenti in situazione di grave di disagio socio-psicologico e relazionale, a grave rischio di emarginazione, maltrattamento, abuso, devianza, anche sottoposti a provvedimenti civili, amministrativi e penali, condividendo un percorso di analisi, ricerca e sperimentazione di servizi innovativi rivolti alla prevenzione primaria e secondaria ed alla cura del disagio psico-sociale.

I dati acquisiti

Al fine di poter provvedere ai servizi che la Cooperativa si prefigge vengono acquisiti una serie di dati personali e sensibili che potremmo distinguere in:

1) DATI ACQUISITI PER LA GESTIONE BUROCRATICA AMMINISTRATIVA E DI GESTIONE DELL'ATTIVITA'

2) DATI ACQUISITI PER LA GESTIONE DELL'OSPITE

Nei primi ricadono perlopiu' dati anagrafici e fiscali, ossia dati trattati per :
a.gestione del personale, **b.** contratti di consulenza, **c.** Convenzioni con Enti, **d**. Contratti con manutentori, **e.** Istituti Bancari, **f.** Istituti di Assicurazione.

Nei secondi ricadono invece tutti i dati anagrafici e sensibili acquisiti per la gestione del servizio erogato all'ospite, ossia trattati per:
a.Contratto d'ingresso sottoscritto per l'ospite da parte di genitori, tutori, Amministratori di Sostegno, **b.** tenuta del PEI

Violazione dei dati personali

In caso di violazione della sicurezza dei dati (data breach) che può avvenire per :

1) Accesso e divulgazione (Confidentiality breach)
2) Alterazione (Integrity breach)
3) Perdita o distruzione (Availability breach)

e in base a quanto stabilito dall'art. 33 del GDPR, la Cooperativa Sociale Optimus informerà della violazione l'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza, salvo i casi in cui vi sia una scarsa probabilità che la violazione diventi un rischio per i diritti e le libertà delle persone fisiche interessate. Se per qualche ragione vi sia un ritardo nella comunicazione, il titolare lo giustificherà.

Analisi del Rischio

Premesso che i dati acquisiti saranno trattati in modalità :

a. CARTACEA
b. INFORMATICA e SITO INTERNET

e che i rischi in cui si incorre sono (DATA BREAK):

a. PERDITA DEI DATI
b. SOTTRAZIONE DEI DATI

e che questi possano di conseguenza ricadere nella gestione/utilizzo di soggetti terzi che non hanno il consenso informato dell'interessato, Titolare e Responsabile del Trattamento intendono adottare le seguenti misure :

DATI TRATTATI IN MODALITA' CARTACEA	Tutti i dati acquisiti (Amministrativi e di gestione dell'ospite e anagrafiche) si trovano nell'ufficio della Cooperativa, locale che rimane chiuso a chiave terminato l'orario d'ufficio e altrimenti presenziato dagli incaricati, nel quale si trova un armadio sempre chiuso. Le chiavi dell'armadio contenente la documentazione sono nella disponibilità dei soli incaricati dopo la chiusura degli archivi.

DATI TRATTATI IN MODALITA' INFORMATICA	Entrambi i PC della Cooperativa posizionati negli uffici oltre al PC portatile in dotazione al Responsabile del Trattamento hanno una Password di accesso che viene periodicamente variata (circa una volta al mese) ed ogni qualvolta per un sospetto di intrusione se ne ravvisi la necessità **La Password di accesso ai PC** sono nella disponibilità del Titolare dei Dati, del Responsabile del trattamento, della Responsabile di struttura Dr.ssa Sara Orlando (incaricata al trattamento e all'accesso dopo la chiusura degli archivi, del Direttore Dott. Davide Panepinto (incaricato al trattamento e all'accesso dopo la chiusura degli archivi), dell'amministrativa Dr.ssa Eliana Torsa (incaricata) **L'accesso al cloud** è stato autorizzato esclusivamente a: Davide Panepinto. La Revoca degli accessi con Password sia dei PC che del Cloud può avvenire in qualsiasi momento **SITO WEB:** l'informativa completa è anche disponibile on line sul nostro sito www.cooperativasocialeoptimus.it, dove è stato creato apposito link che rimanda all'informativa. Anche attraverso le comunicazioni elettroniche, quali e mail, è possibile accedere al link sopra indicato, per una maggiore diffusione dell'informativa.

Considerato il tipo di attività, si può ben comprendere che i fascicoli sanitari ed educativi dei nostri ospiti, seppur assicurati all'interno di un locale chiuso a chiave e in un armadio a sua volta chiuso a chiave sono e devono rimanere a disposizione dell'intera equipe multidisciplinare, operante all'interno della Cooperativa, in ogni momento. Per questa ragione, Titolare e Responsabile del trattamento hanno optato per incaricare tutti i componenti dell'equipe. Oltre a quanto descritto, per informazione, nella lettera di nomina "incaricato" si ritiene necessario un momento di **formazione e sensibilizzazione** degli incaricati al fine di responsabilizzarli nella gestione dei dati che trattano durante la loro attività lavorativa in Cooperativa e sappiano garantirne la sicurezza.

Inoltre, a maggior tutela della salvaguardia dei dati, della buona pratica svolta in tal senso e della trasparenza con la quale la Cooperativa intende lavorare anche in campo privacy, si decide di introdurre la figura del DPO. Con la nomina di questa figura, che si individua nella persona della Dr Davide Panepinto; il Titolare e il Responsabile del Trattamento intendono condividere e promuovere azioni migliorative, monitorare l'operato degli incaricati in tema di salvaguardia dei dati anche attraverso la formazione periodica, richiedere consulenza nella gestione di eventuali rischi rilevati.

Salvataggio dei dati

Il salvataggio dei Dati sensibili avviene in **cloud**. Riteniamo che altri sistemi di backup non sarebbero sicuri al 100% . Ad esempio se si salvassero i dati su un hard disk esterno bisognerebbe chiuderlo a chiave in cassaforte e garantirne la sorveglianza 24 ore su 24.

Cloud, per noi nello specifico Echos, consente a noi e solo a noi incaricati di accedere ai dati in qualsiasi momento senza l'ansia del data breach. **SEMPLICI** ma
IMPORTANTI ACCORGIMENTI:

1) Accedere al **Cloud** senza farsi "rubare la password"
2) Consultare i dati lontano da chi non è incaricato della salvaguardia degli stessi
3) Cambiare spesso la Password

Distruzione dei dati

La distruzione dei dati potrà avvenire nel caso di richiesta dell'interessato (nel rispetto del diritto all'oblio), nel caso questi non siano più necessari ai fini dell'attività.

DISTRUZIONE DATI CARTACEI	VIENE EFFETTUATA ATTRAVERSO L'UTILIZZO DEL DISTRUGGI DOCUMENTI
DISTRUZIONE DATI INFORMATICI	CANCELLAZIONE DAL CLOUD E DAGLI ARCHIVI INFORMATICI

CONSIDERAZIONI

Al fine di rispettare le normative vigenti e non incorrere in sanzioni, la Cooperativa ha già provveduto alla stesura della nuova documentazione privacy. Tutta la documentazione è disposta in apposito faldone conservato nell'ufficio della Cooperativa a disposizione per eventuali controlli da parte dagli organi competenti. La Cooperativa ha provveduto, nei termini di legge previsti, alla consegna della documentazione privacy (informativa, consenso e atti di nomina) e relativa presa visione e successiva firma da parte delle persone incaricate al trattamento dei dati.