PROCEDURA PER LA CONFORMITÀ AL GDPR

REGOLAMENTO UE679/2016
D.LGS. 101/2018

BIANALISI S.P.A.
analisi mediche

Versione del Documento

Redatto da	Data di Revisione	Motivo del Rilascio
DPO - Dott.ssa Serenella Saccon	07/07/2020	1° Rilascio

Approvatori del Documento

Versione Documento	Funzione Aziendale	Data
V1	Direzione Aziendale	07/07/2020

Registro Modifiche di Versione

Versione Documento	Sezione Modificata	Descrizione della Modifica

Indice generale

1.Scopo e normativa di riferimento

Scopo della presente procedura è di pianificare gli adempimenti necessari per l'adeguamento al GDPR e per il mantenimento delle condizioni di conformità, fornire istruzioni ai soggetti coinvolti e determinare modalità di lavoro.
La normativa di riferimento è la seguente :

- Regolamento UE679/2016
- D.Lgs. 101/2018

2. Campo di applicazione e comunicazione

La procedura è da applicarsi in ogni sede lavorativa ed è destinata a tutti coloro che operano per il Titolare di trattamento a qualunque titolo. Come indicato nei paragrafi successivi, ogni soggetto ha precisi doveri e attività da svolgere.

3. Soggetti

Tutti coloro che lavorano a qualunque titolo per il Titolare di trattamento sono coinvolti negli adempimenti richiesti per raggiungere e mantenere la conformità al GDPR ed ognuno ha responsabilità in merito. I soggetti sono individuati come segue :

Titolare di trattamento
L'azienda nel suo complesso individuata come ragione sociale. Il Titolare è responsabile verso gli interessati.

Referente interno
La normativa europea non prevede più un responsabile del trattamento dati interno quale "braccio operativo" del titolare di trattamento ma è utile che in azienda ci sia un referente per la materia in questione, che vigili sull'operato degli incaricati/autorizzati e tenga sotto controllo la documentazione. Il referente non va confuso con il responsabile individuato dal regolamento europeo, quest'ultimo infatti esegue trattamenti per conto del titolare e corrisponde al responsabile esterno già previsto in precedenza dalla normativa italiana. Il referente può appoggiarsi all'RPD per ogni questione e supportare l'RPD stesso nella diffusione di documenti o nella raccolta di informazioni.

Incaricati o autorizzati al trattamento
Tutto il personale interno (dipendenti, autonomi, professionisti, collaboratori, stagisti ecc.) che in ogni modo o per qualunque motivo debba trattare dati deve essere individuato come autorizzato al trattamento. La normativa europea non cita espressamente la lettera di incarico ma è previsto che i soggetti siano individuati, formati ed autorizzati e quindi un documento comprovante tali azioni deve essere prodotto. Si continua perciò ad incaricare il personale specificando mansioni ed operazioni consentite o non consentite ove utile.

Responsabile esterno del trattamento
Il responsabile esterno è una ragione sociale (quindi un'azienda) alla quale il titolare di trattamento comunica dati perché il responsabile esegua trattamenti specifici (meglio se indicati in contratti o incarichi). Ogni responsabile deve essere nominato in forma scritta.

Responsabile protezione dati
Il soggetto RPD o DPO (Data protection officer) è nominato dal titolare in determinati casi previsti dalla normativa. Se presente, fornisce consulenza e soluzioni a problematiche o dubbi in materia di trattamento dati, controlla la correttezza e completezza della documentazione, esegue le attività che ritiene utili per consentire al titolare la piena conformità e fa da contatto in caso di intervento del Garante per la protezione dei dati.

4. Adempimenti del Titolare del Trattamento

Il Titolare di trattamento è responsabile per l'attuazione degli adempimenti previsti dal GDPR.

Ha doveri e responsabilità nei confronti di tutti gli interessati, quindi di tutte le persone di cui tratta dati per qualsiasi motivo (clienti, dipendenti, professionisti, fornitori ecc.).

Gli adempimenti individuati sono di diversa tipologia :

Informazione e consensi	• informare gli interessati • fornire agli interessati risposte e possibilità di esercitare i diritti ex art. 15 GDPR • raccogliere il consenso degli interessati
Incarichi e nomine	• individuare il proprio organigramma interno in materia di privacy con incarichi specifici • individuare i responsabili esterni con nomine specifiche • formare i soggetti che eseguiranno i trattamenti • nominare il soggetto RPD • esaminare ed eventualmente accettare la nomina quale responsabile esterno o provvedere all'assunzione di responsabilità ove necessario
Operatività pratica	• pianificare le operazioni considerando il principio privacy by default e by design • formare gli operatori • assicurarsi che gli strumenti e le modalità di trattamento e conservazione siano sicuri • raccogliere soltanto i dati necessari • effettuare i trattamenti correttamente • conservare i dati utili e per il tempo necessario • prevedere tempi e modalità di distruzione dei dati • intervenire in caso di data breach
Documentazione	• realizzare e mantenere i documenti richiesti dalla normativa • eseguire una valutazione d'impatto all'inizio del trattamento o alla variazione di elementi fondamentali • revisionare dati e documenti periodicamente

4.1 Informazione e consensi

Il Titolare fornisce agli interessati un'informativa che deve essere chiara e completa. Deve contenere tutti gli elementi che consentano all'interessato di fornire un consenso consapevole al trattamento, quindi dovrà indicare chi tratta i dati, chi ne è responsabile, qual è lo scopo, informazioni in relazione alle modalità, alle misure di sicurezza, al luogo di conservazione, all'esercizio dei diritti.
Rif. Documenti : Modelli informativa e consenso

4.2 Incarichi e nomine

L'incarico destinato agli operatori deve contenere la mansione svolta, che implica le attività indicate nel mansionario. Ove necessario si indichino anche le condizioni particolari come l'accesso a sezioni di database o abilitazione a comunicazioni con la PA.

La nomina ai responsabili esterni deve far riferimento al contratto nel quale si descrivono i trattamenti richiesti e le modalità, nonché gli obblighi previsti dalla normativa.

Altri Titolari di trattamento possono nominare l'azienda come responsabile esterno, le nomine ricevute devono essere esaminate per assicurarsi che siano giustificate e che il contenuto sia corretto. In taluni casi i Titolari di trattamento tardano eccessivamente a nominare l'azienda che, nel frattempo, si trova ad eseguire i trattamenti comunque. In alcuni casi risulta quindi utile assumere il ruolo di responsabile comunicandolo al titolare di trattamento cliente.

Rif. Documento : Nomina RPD (con delega e ricevuta del Garante), Modelli incarico, nomina responsabile esterno, nomina amministratore di sistema, assunzione incarico quale responsabile esterno, Organigramma, Mansionario amministrativo

4.3 Organizzazione del lavoro

Il Titolare deve pianificare le operazioni di trattamento tenendo in considerazione la protezione dei dati quale elemento fondamentale durante il trattamento e obiettivo della conservazione. La protezione dei dati quindi deve essere un elemento della pianificazione e della realizzazione degli strumenti (privacy by design) e deve essere sempre presente come elemento da rispettare durante le attività (privacy by default).
Gli operatori che eseguono i trattamenti devono essere formati, devono ricevere le informazioni e le istruzioni necessarie per operare correttamente. Le modalità della formazione sono lasciate alla discrezionalità del Titolare di trattamento.
Gli strumenti sono gli elementi hardware e software descritti negli asset aziendali all'interno del registro elettronico o comunque inventariati in specifica documentazione alla quale il registro può fare riferimento. Ogni strumento deve essere valutato sotto l'aspetto della sicurezza dei dati prima di effettuarne l'acquisto, l'installazione, l'utilizzo.
Le operazioni pratiche di raccolta dei dati devono essere organizzate in modo da raccogliere effettivamente soltanto i dati necessari per le finalità predeterminate. Le procedure stabilite per i trattamenti dovranno assicurare la riservatezza e l'integrità dei dati, da mantenersi anche in fase di conservazione. Ove possibile (secondo la tipologia di attività svolta dal Titolare), dovranno essere definiti i termini di conservazione e le modalità di distruzione dei dati. Ove la distruzione non sia possibile si prevederanno modalità di conservazione estremamente sicure e si assicurerà la riservatezza delle informazioni per tutto il tempo di conservazione.
Rif. Documenti : Istruzioni Operative per gli incaricati/autorizzati, Registro dei trattamenti in qualità di responsabile

4.3.1 Doveri di conservazione in relazione ai dati e misure di sicurezza

Il Titolare di trattamento, tramite i propri incaricati, provvede alla corretta conservazione dei dati e dei supporti cartacei ed informatici sui quali sono stati registrati. In relazione ai dati si considerano i dati che al momento della raccolta vengono inseriti in database del software di gestione e i dati prodotti o raccolti che vengono conservati in file locali.

4.3.1 Dati in database di software di gestione

Il software principale di gestione operativa fa confluire i dati in un datacenter sicuro (certificazione ISO 27001) gestito dal fornitore S.P.E. Sistemi e Progetti Elettronici s.a.s. La certificazione assicura i requisiti richiesti dalla normativa compreso il backup.

4.3.2 Dati conservati in locale

Eventuali dati conservati in locale non sono da considerarsi sicuri in quanto manca, al momento, una corretta gestione del sistema informatico presente presso ogni sede lavorativa. Il fornitore di riferimento (S.P.E. Sistemi e Progetti Elettronici s.a.s.) fornice software di protezione antivirus e protezione antivirus e antimalware sulle caselle email.

4.4 Data breach

In caso di violazione dei dati (data breach) è necessario seguire le istruzioni indicate nella relativa procedura provvedendo al più presto alle azioni immediate che pongono termine all'evento e alle azioni successive di comunicazione entro le 72 ore. Le violazioni devono essere indicare nel registro delle violazioni (incluso nel registro dei trattamenti), che abbiano dato adito a comunicazione oppure no.

Rif. Documento : Procedura Data Breach

4.5 Documenti

4.5.1 Documentazione da produrre

L'applicazione del GDPR richiede la produzione di documentazione cartacea e digitale, destinata a diverse tipologie di interessati e ad uso interno.

I seguenti documenti sono destinati a utenti/clienti/pazienti, stampati direttamente dal software di gestione al momento dell'accettazione per essere firmati dall'interessato e poi conservati in cartaceo originale :

- informativa sul trattamento dati

I seguenti documenti sono destinati al personale interno, stampati al momento dell'inizio del rapporto lavorativo per essere firmati dall'interessato e poi conservati in cartaceo originale :

- informativa sul trattamento dati
- incarico per il trattamento dati
- liberatoria per l'uso di immagini e materiali audio e video

I seguenti documenti sono destinati a ragioni sociali diverse, stampati al momento dell'individuazione della ragione sociale quale fornitore di servizi per essere firmati da soggetto con potere di firma e poi conservati in cartaceo originale :

- nomina quale responsabile esterno del trattamento

I seguenti documenti sono prodotti internamente ed utilizzati per il mantenimento della conformità al GDPR :

- Registro dei trattamenti in qualità di titolare del trattamento
- Registro dei trattamenti in qualità di responsabile del trattamento
- Valutazione d'impatto DPIA
- Procedura data breach
- manuale ad uso degli incaricati

4.5.2 Documentazione da conservare

La normativa richiede che la documentazione cartacea presente in azienda venga conservata in sicurezza, con accesso consentito soltanto al personale autorizzato al relativo trattamento. Si possono distinguere i documenti prodotti per la conformità al GDPR dai documenti presenti per le attività aziendali.

In relazione ai **documenti di conformità** il referente interno dovrà accertarsi di conservare in specifica cartella sotto il suo controllo i seguenti file (documenti in formato digitale) :

- Registro dei trattamenti in qualità di titolare del trattamento
- Registro dei trattamenti in qualità di responsabile del trattamento
- Valutazione d'impatto DPIA
- Procedura data breach
- Istruzioni al personale interno per la materia specifica (un modello esemplificativo), se le istruzioni sono parte delle procedure interne si possono conservare con le procedure
- Note sulla formazione del personale in materia di privacy (eventuali corsi, materiale informativo, verbali di riunione ecc.)
- Testo dell'informativa inviata a fornitori se inviata (un modello esemplificativo)
- Mail di conferma della comunicazione al Garante per la protezione dati del nominativo del RPD
- Modelli di ogni testo prodotto in materia di trattamento dati

dovrà inoltre accertarsi di conservare in specifico faldone sotto il suo controllo i seguenti documenti in formato cartaceo :

- Informative al personale interno con consenso firmate
- Incarichi al personale interno firmati
- Nomine a responsabili esterni firmate
- Nomine che il centro ha ricevuto quale responsabile esterno per clienti aziendali firmate
- Designazione del Responsabile Protezione Dati firmata
- Stampa della mail di conferma della comunicazione al Garante per la protezione dati del nominativo del RPD, allegata alla designazione.

I seguenti documenti cartacei possono essere conservati con diversa modalità purché il referente aziendale ne abbia conoscenza e controllo :

- Informative con consenso firmate da clienti/pazienti (possono essere conservate anche nei singoli fascicoli dei pazienti o in specifico archivio dedicato)

In relazione ai **documenti aziendali**, il referente interno dovrà accertarsi che le modalità di conservazione (digitali o cartacee) siano sicure e assicurino la riservatezza e l'integrità dei dati. In elenco esemplificativo :

- Organigramma interno
- Mansionario funzionale
- Contratti con professionisti, fornitori, clienti persone giuridiche
- Procedure interne di lavoro, regolamenti
- Documenti inerenti i rapporti di lavoro con dipendenti
- Documenti inerenti le prestazioni all'utenza (impegnative, referti, reperti ecc.)

Rif. Documento : Scheda documenti in cartaceo e in digitale, Titolario e Massimario di scarto Regione Lombardia, Registro dei trattamenti

4.5.3 Valutazione d'impatto

Quando il trattamento dei dati personali è suscettibile di provocare un rischio elevato per i diritti e le libertà delle persone fisiche è necessario effettuare una valutazione d'impatto (DPIA) che comprenda :

• una descrizione delle operazioni di trattamento previste e delle finalità di trattamento;
• una valutazione della necessità e della proporzionalità del trattamento;
• una valutazione dei rischi per i diritti e le libertà delle persone;
• le misure previste per affrontare i rischi o dimostrare il rispetto del regolamento;
• l'eventuale rispetto di un codice di condotta.

La valutazione è stata effettuata e viene conservata nell'ultima versione.
Rif. Documento : valutazione d'impatto DPIA

5. Doveri del Referente interno

Il referente interno è il soggetto individuato dal Titolare del trattamento per l'esecuzione pratica degli adempimenti. Ha il compito di fare da punto di riferimento per gli incaricati, vigilare sull'applicazione della procedura e sull'esecuzione dei compiti degli operatori, controllare la presenza e l'aggiornamento dei documenti, eventualmente raccogliere le richieste degli interessati.

6. Adempimenti del Titolare in qualità di Responsabile del trattamento

In qualità di responsabile del trattamento, l'azienda esegue trattamenti per la clientela (persone giuridiche), necessari per l'esecuzione dei contratti in essere. L'elenco delle nomine ricevute e dei trattamenti eseguiti viene registrato nel registro in qualità di responsabile. I dati trattati per conto di altri titolari sono protetti con le stesse misure di protezione applicate ai dati trattati per proprie attività.

7. Adempimenti del Responsabile Protezione Dati

L'RPD resta a disposizione del Titolare del trattamento e di tutti coloro che per suo conto trattano dati per fornire risposte e consulenza e deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. Funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le

questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti, l'RPD è tenuto al segreto o alla riservatezza.

8. Adempimenti degli incaricati o autorizzati al trattamento

8.1 Area amministrativa Front Office

Nell'ambito del trattamento dati, il personale con mansioni relative all'accettazione ha il compito di :

- consegnare le informative all'utenza e raccogliere il consenso al trattamento
- raccogliere i dati necessari ed inserirli in database
- elaborare fatture e consegnarli all'utenza
- consegnare referti e risultati all'utenza
- utilizzare la modulistica predisposta
- seguire le procedure e le istruzioni ricevute

Rif. Documenti : Avviso per ritiro tramite totem, Nota referti HIV, Procedure e gestione ROL

8.1 Area amministrativa Back Office e contabilità

Nell'ambito del trattamento dati, il personale con mansioni di back office ha il compito di :

- elaborare dati ed informazioni trattando dati dell'utenza
- seguire le procedure e le istruzioni ricevute

Nell'ambito del trattamento dati, il personale con mansioni amministrative di contabilità ha il compito di :

- elaborare dati ed informazioni trattando dati dell'utenza
- elaborare dati ed informazioni trattando dati di clienti, fornitori, personale interno
- seguire le procedure e le istruzioni ricevute

8.2 Area Operativa

Nell'ambito del trattamento dati, il personale operativo ha contatto diretto con pazienti e personale interno. Ha il compito di operare correttamente seguendo le istruzioni ricevute e mantenendo la riservatezza sulle informazioni.

9. Documentazione

Di seguito viene riportata la documentazione a supporto della procedura per la conformità sopra descritta:

Scheda documenti in cartaceo e in digitale
Procedura Data Breach
Nomina RPD
Comunicazione RPD - delega
DPIA
Istruzioni Operative per gli incaricati/autorizzati
Modello informativa e consenso per il personale interno
Modello informativa e consenso per gli utenti/clienti/pazienti
Modello informativa e consenso per gli utenti/clienti/pazienti con minori o interdetti
Modello incarico
Modello nomina responsabile esterno
Modello nomina amministratore di sistema
Modello assunzione incarico quale responsabile esterno
Avviso per ritiro tramite totem
Nota referti HIV

Procedure e gestione ROL
Registro dei trattamenti e Registro dei trattamenti in qualità di responsabile
Organigramma
Mansionario
Regolamento UE679/2016
D.Lgs. 101/2018
Titolario e Massimario di scarto Regione Lombardia