Preambolo: l'obiettivo di questo documento è fornire informazioni sul GDPR e illustrare i suoi effetti su Unilabs. Pur avendo ad oggetto alcuni concetti ed effetti giuridici, non deve essere considerato un parere legale, né una raccomandazione basata su un'interpretazione giuridica particolare. Le normative nazionali (ad esempio, quelle sulla protezione dei dati o il diritto del lavoro) o restrizioni relative all'ambito sanitario possono incidere sull'interpretazione delle informazioni fornite.
Per favore, rivolgetevi al *team* di progetto GDPR di Unilabs al seguente indirizzo email gdprproject@unilabs.com per ogni dubbio interpretativo su quanto sotto esposto o per ogni altra domanda.

Concetti generali del GDPR

1. Che cos'è il GDPR?

Il GDPR (**G**eneral **D**ata **P**rotection **R**egulation o Regolamento Generale sulla Protezione dei Dati) è il nuovo riferimento normativo europeo per la protezione dei dati personali dei residenti nell'UE. Armonizza le leggi sulla protezione dei dati in tutta l'UE e ha per scopo quello di proteggere i diritti fondamentali e la libertà delle persone fisiche, e in particolare il loro diritto alla protezione dei dati personali.
Il regolamento entra in vigore il 25 maggio 2018.

2. Che cosa sono i dati personali?

Qualsiasi informazione riferita a una persona fisica o a un "interessato" che possa essere utilizzata per identificare la persona direttamente o indirettamente. Può essere qualsiasi cosa: un nome, una foto, un indirizzo *email*, riferimenti bancari, post sui *social-network*, informazioni sanitarie, o l'indirizzo IP di un *computer*.

3. Cos'è un "interessato"?

Qualsiasi persona fisica che possa essere identificata direttamente o indirettamente. Per Unilabs un interessato può essere un dipendente, un paziente, un potenziale cliente, un cliente o un altro professionista sanitario, un candidato o un fornitore (se si tratta di persone fisiche, non di persone giuridiche). Gli interessati sono coloro che il GDPR tutela e ai quali fornisce i mezzi per conoscere e verificare come i loro dati personali vengono trattati.

4. Cos'è il trattamento di dati personali?

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, su dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica e l'uso di dati.

5. Chi è tenuto al rispetto del GDPR?

Qualsiasi struttura od organizzazione che tratti dati di residenti nell'UE.

6. Quali sono le conseguenze nel caso di non rispetto del GDPR?

Le organizzazioni possono essere multate con un importo fino al 4% del fatturato mondiale annuo o fino a 20 milioni di Euro, se superiore.

7. Quali sono le obbligazioni di un'organizzazione secondo il GDPR?

Un'organizzazione soggetta al GDPR deve trattare i dati personali:

- In modo lecito e corretto.
- Per finalità determinate, esplicite e legittime.
- Utilizzando dati personali adeguati, pertinenti, limitati, accurati e aggiornati.
- Per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono trattati.
- In conformità ai diritti degli interessati.
- Assicurando un alto livello di sicurezza.
- All'interno dell'Unione Europea, o in conformità alle regole sul trasferimento di dati al di fuori dell'UE.
- In conformità ai registri delle attività di trattamento.

Il GDPR in Unilabs

8. Il GDPR si applica a Unilabs?
Sì, ogni organizzazione Unilabs con sede nella UE, o che tratti dati di residenti nella UE, deve rispettare il GDPR. In pratica, Unilabs ha esteso l'obbligo di rispettare il GDPR a tutte le persone giuridiche del Gruppo, comprese anche le aziende non-UE.

9. In che modo Unilabs è responsabile del rispetto del GDPR?
Ogni persona giuridica in Unilabs deve rispettare il GDPR. Ogni soggetto giuridico deve essere in grado di dimostrare di rispettare il GDPR. Ogni azione eseguita per adeguarsi al GDPR deve essere documentata in modo tale che possa essere verificata dalle autorità di controllo della protezione dei dati.

10. Come il GDPR contribuirà all'attività di Unilabs?
La protezione dei dati non è un concetto nuovo ed è già intrinsecamente parte dell'attività di Unilabs. Rende Unilabs ancor più affidabile e inoltre dà a tutti i soggetti interessati maggiori garanzie circa il fatto che noi ci preoccupiamo dei loro dati.

11. Come Unilabs si sta adeguando al GDPR?
Unilabs sta rafforzando in tutta l'organizzazione processi interni per garantire che tutti i dati personali vengano trattati in base allo standard di protezione più elevato imposto dal GDPR. Ciò comporta:

- Creare un registro relativo a tutte le operazioni di trattamento dei dati.
- Gestire i dati personali durante tutto il loro ciclo vitale per controllarne la raccolta, l'archiviazione, il trattamento, l'accesso, la modificazione e la cancellazione.
- Informare in modo trasparente gli interessati sul trattamento dei loro dati.
- Gestire le richieste degli interessati.
- Aumentare il livello di sicurezza di tutte le attività di trattamento.
- Controllare coloro che trattano i dati attraverso clausole contrattuali adeguate.
- Trasferire in sicurezza i dati fuori dallo Spazio Economico Europeo.
- Notificare ogni eventuale violazione della sicurezza dei dati.
- Inserire in tutte le nuove attività di trattamento i principi di "*privacy by design*" e "*security by default*".
- Valutare l'impatto sulla *privacy* di attività di trattamento ad alto rischio.
- Implementare adeguate misure tecniche e organizzative.

Analogamente alla gestione della qualità, la protezione dei dati richiede uno sforzo continuo per garantire che i processi di cui sopra funzionino correttamente. Per ottenere un'implementazione efficace del GDPR, Unilabs sta mettendo in piedi un'organizzazione, guidata dal Responsabile della Protezione dei dati a livello di Gruppo, per seguire e monitorare il livello di adeguamento al GDPR.

12. Qual è il ruolo del Responsabile del Trattamento dei Dati?
Il Responsabile del Trattamento dei Dati si occupa di informare, verificare il rispetto del GDPR e prestare consulenza a Unilabs. E' inoltre il contatto ufficiale per le autorità di controllo sulla protezione dei dati operanti in tutti i Paesi UE.

13. Il responsabile del Trattamento dei Dati è responsabile in caso di non rispetto del GDPR?
No, la responsabilità finale sta in capo al legale rappresentante di ciascuna persona giuridica (CEO o dirigente della persona giuridica).

14. Ci sono specifici requisiti che Unilabs deve rispettare dal momento che tratta dati riferiti alla salute?
Unilabs tratta dati riferiti alla salute perché la sua attività principale è l'assistenza medica. E' compresa nell'ambito delle eccezioni previste nel GDPR, che in linea generale vieta il trattamento di dati sensibili, come i dati sanitari, a causa dell'alto rischio per i diritti e le libertà fondamentali delle persone.
Ci sono in ogni caso requisiti specifici legati al trattamento di dati relativi alla salute, come ad esempio misure di sicurezza aggiuntive.
Al contempo, il trattamento di dati relativi alla salute, per scopi diversi dall'assistenza medica, deve essere attentamente valutato e ottenere l'autorizzazione del soggetto interessato. Devono in ogni caso essere rispettati gli stessi requisiti previsti dal GDPR.

15. Unilabs è titolare del trattamento o responsabile del trattamento?
Il GDPR definisce "titolare del trattamento" il soggetto che determina le finalità, le condizioni e i mezzi del trattamento dei dati personali, mentre definisce "responsabile del trattamento" il soggetto che tratta dati personali per conto del titolare del trattamento.
Per la maggior parte delle attività di trattamento di dati, Unilabs è titolare del trattamento, dal momento che definisce finalità, condizioni e mezzi del trattamento di dati personali, anche quando i dati vengono raccolti da un altro soggetto (per esempio, un ospedale). Un esempio di responsabile di trattamento che agisce per conto di Unilabs può essere un fornitore IT che ospiti server di applicazioni Unilabs nel proprio *data-center*.
In alcuni casi la decisione di agire come titolare o responsabile è di carattere strategico, dettata dalle relazioni di Unilabs con altri enti (soggetti interni o esterni che svolgano il ruolo complementare rispetto a quello svolto da Unilabs).

16. Se Unilabs si avvale di responsabili del trattamento dei dati, come può garantire che essi rispettino il GDPR?
Il GDPR impone maggiori obblighi ai responsabili del trattamento dei dati, che possono essere tenuti a rispondere di danni nei confronti degli interessati. Vi sono inoltre alcune statuizioni che devono obbligatoriamente essere contenute nei contratti che regolano i rapporti tra Unilbas e i suoi responsabili del trattamento dei dati.

17. Come dobbiamo gestire dati che appartengono a un'altra azienda?
Il GDPR non contiene alcun riferimento alla nozione di proprietà dei dati e si applica ai titolari del trattamento o ai responsabili del trattamento di dati personali. Ciò che può cambiare è il modo in cui i dati vengono raccolti (direttamente dall'interessato o indirettamente).

18. Se il trattamento è limitato a informazioni di contatto di tipo professionale (email, telefoni), occorre rispettare il GDPR?

Il GDPR si applica a tutti i dati personali, e non fissa una gerarchia di dati che debbano in maggiore o minore misura rispettarlo. Spetta a ciascuna azienda definire i livelli di rischio accettabili e documentarli, così da poter giustificare eccezioni in caso di controlli da parte delle autorità di controllo.

19. Unilabs deve cifrare tutti I dati per rispettare il GDPR?

Il GDPR non è un referente di regole tecniche o di sicurezza, ma costituisce la cornice all'interno della quale gestire i dati dati personali. Richiede l'implementazione di misure tecniche e organizzative per garantire un adeguato livello di sicurezza. Sarà "adeguato" il livello che permetta di raggiungere un punto di equilibrio tra costi di implementazione della misura, scopo, contesto e finalità del trattamento, e rischio in caso di violazione della sicurezza dei dati.

In alcuni casi, ad esempio quando si trattano dati sensibili (come quelli sanitari), il GDPR richiede espressamente che tali dati vengano pseudonomizzati e cifrati.

20. Unilabs deve ottenere il consenso dagli interessati per trattarne i dati personali?

Non necessariamente. Il consenso è una base giuridica per il trattamento dei dati personali, ma ve ne sono altre, come ad esempio:

- l'esecuzione di un contratto;
- l'adempimento di un obbligo legale;
- la protezione degli interessi vitali dell'interessato;
- l'esecuzione di compiti necessari per la tutela del pubblico interesse;
- il legittimo interesse perseguito dal titolare del trattamento.

La base giuridica è definita dal titolare del trattamento. Se Unilabs è titolare del trattamento e se ritiene che il trattamento sia giustificato da una delle basi giuridiche di cui sopra, allora il consenso non è richiesto.

21. Unilabs deve ottenere il consenso dagli interessati per trattarne i dati sanitari?

Non sempre. La base giuridica per il trattamento dei dati sensibili viene definiao dal titolare del trattamento dei dati. Se il trattamento di dati sensibili è necessario per formulare una diagnosi medica, il consenso dell'interessato non è necessario.

22. L'interessato come deve prestare il consenso?

Il consenso deve essere prestato in maniera libera, specifica, informata e inequivocabilmente conforme ai desideri della persona. Il GDPR pone a carico del titolare del trattamento l'onere di dimostrare che il consenso è stato prestato.

A seguire alcuni esempi di consenso prestato non validamente:

- Silenzio.
- Preselezione di caselle.
- Inattività.
- Rapporto di subordinazione.
- Contratto di affiliazione.
- Evidente squilibrio tra titolare del trattamento e interessati.

23. Che cos'è il periodo di conservazione dei dati personali?
Il GDPR non definisce un periodo di conservazione specifico per ciascun tipo di dato. Ma il GDPR prevede che i dati siano cancellati una volta concluso il periodo di conservazione o quando il trattamento non sia più necessario in considerazione dello scopo per il quale i dati sono stati raccolti o trattati.

24. Il GDPR può entrare in conflitto con altri obblighi di conservazione?
Il periodo di conservazione è solitamente fissato dalla legislazione nazionale. Il GDPR non entra in conflitto con la legislazione nazionale, poiché prevede che i dati debbano essere cancellati dopo che il periodo di conservazione si è concluso o quando lo scopo del trattamento dei dati non esiste più.

25. I trasferimenti di dati sono consenti?
I trasferimenti di dati, vale a dire i trasferimenti di dati al di fuori dello Spazio Economico Europeo, sono possibili nei seguenti casi:
- Il Paese di destinazione è considerato dall'UE come in grado di fornire un adeguato livello di protezione: come nel caso della Svizzera.
- Il trasferimento è realizzato con le garanzie appropriate, che includono:
    - Applicare un meccanismo di protezione dei dati, come il c.d. *Privacy Shield* (quando il Paese di destinazione siano gli Stati Uniti).
    - Introdurre clausole contrattuali standard.
    - Stabilire regole aziendali vincolanti.
    - Approvare un codice di condotta.
    - Approvare un meccanismo di certificazione.

26. Il GDPR vieta di inviare dati personali o riferiti alla salute fuori dal Paese?
Il trasferimento di dati è consentito a certe condizioni, illustrate alla domanda 2525. In ogni caso, nel singolo Paese possono essere previste discipline specifiche in tema sanitario che impongano restrizioni specifiche in materia di dati sanitari.

27. Il trasferimento di dati dalla Svizzera è considerato trasferimento di dati?
No, si è in presenza di un trasferimento internazionale di dati personali quando i dati vengano trasferiti da un soggetto giuridico con sede nello Spazio Economico Europeo a un soggetto giuridico con sede fuori dallo Spazio Economico Europeo.

Il GDPR per i dipendenti Unilabs

28. Quali effetti avrà GDPR per i dipendenti Unilabs?
Il GDPR si applicherà a ogni dipendente Unilabs che raccolga o tratti dati personali, per esempio di pazienti o di altri dipendenti. Come indicato nei precedenti paragrafi, Unilabs deve rispettare alcune obbligazioni previste dal GDPR, in generale attraverso l'implementazione di processi conformi al GDPR stesso (cfr. domanda 1111). A qualsiasi persona giuridica, Stato o dipartimento appartengano, i dipendenti Unilabs dovranno attenersi a questi processi. Unilabs offrirà a breve programmi formativi per assicurare che tutti i dipendenti sappiano come applicare tali processi.
Inoltre, i dipendenti Unilabs sono interessati per quanto concerne le operazioni di trattamento dei loro dati personali (come, ad esempio, nel caso delle attività necessarie alla gestione delle risorse umane). Unilabs dovrà informare i dipendenti circa tali attività di trattamento e circa i diritti loro spettanti.

29. I dati riferiti alla salute sono dati personali?
Sì, se possono identificare direttamente o indirettamente un individuo. L'identificazione di un paziente che è associata al nome del paziente o ad altri dati identificabili rappresenta un dato personale. Se tale possibilità di associazione non sussiste, allora non si è in presenza di dati personali secondo il GDPR. Bisogna tuttavia prestare attenzione a che altre normative riferite alla salute non si applichino all'uso di dati sanitari.

30. I dati cifrati o resi anonimi sono dati personali?
Se i dati cifrati o resi anonimi sono stati ottenuti a partire da dati personali e se questi ultimi possono essere associati ai primi, allora sì.

31. Il GDPR si applica a dati personali sottoposti a trattamento non automatizzato?
Sì, si applica.

32. I dati confidenziali sono dati personali?
Non necessariamente. Dati come, ad esempio, quelli relativi a costi, a risultati finanziari o a un piano strategico possono essere considerati confidenziali, ma possono non contenere dati personali. Sebbene a tali dati si applichino specifici requisiti di riservatezza (*policy* aziendali), il GDPR non si applica ai dati confidenziali.

33. Il GDPR vieta di comunicare dati personali al telefono?
No, ma il GDPR impone che i dati personali, soprattutto quando vi si ha un rischio elevato per i diritti fondamentali e la libertà delle persone, siano protetti con adeguate misure di sicurezza. Questa domanda riguarda più le politiche di riservatezza che stabiliscono quali informazioni possono essere comunicate, a chi e come.