Ordine dei Medici Chirurghi e Odontoiatri della Provincia di Forlì-Cesena

GDPR

General Data Protection Regulation
GDPR - UE 2016/679

Ragione Sociale: **Ordine dei Medici Forlì e Cesena**

Codice Fiscale: **80001750407**

Indirizzo: **Viale Italia 153**

Comune: **FORLI'**

Provincia: **FC**

Contenuti:

- Questionario GDPR
- Registro trattamento Dati GDPR
- Organigramma
- Istruzioni gestione Data Breach

Data ultimo aggiornamento: 10/09/2025

Premessa.

Così come stabilito dall'art.4 Reg. UE 679/2016, si precisa che ai fini del presente registro s'intende per:

1) **«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;

2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) **«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;

4) **«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;'' I dati cc.dd. pseudonimi sono quei dati personali nei quali gli elementi identificativi sono stati sostituiti da elementi diversi, quali stringhe di caratteri o numeri (hash), oppure sostituendo al nome un nickname, purché sia tale da rendere estremamente difficoltosa l'identificazione dell'interessato. Ovviamente il soggetto che detiene la chiave per decifrare i dati (cioè collegare l'elemento pseudonimo al dato personale) deve garantire adeguate misure contro possibili abusi.
I dati pseudonimi, a differenza di quelli anonimizzati, sono comunque dati personali (in quanto consentono l'identificazione della persona, anche se indirettamente, tramite incrocio con altre informazioni), anche se soggetti ad una tutela ridotta rispetto ai dati personali veri e propri.

5) **«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;

6) **«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;

7) **«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;

8) **«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;

9) **«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;

10) **«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;

11) **«violazione dei dati personali»**: 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;

12) **«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;

13) **«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;

14) **«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;

15) **«stabilimento principale»**:

- per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

- con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

16) **«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, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

17) **«impresa»**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

18) **«norme vincolanti d'impresa»**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

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

20) **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

- il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
- gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
- un reclamo è stato proposto a tale autorità di controllo;

21) **«trattamento transfrontaliero»**:

- 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
- 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''

22) **«dati anonimizzati»:** sono quei dati che sono stati privati di tutti gli elementi identificativi; non sono perciò considerabili quali dati personali e non sono soggetti alle norme a tutela dei dati personali.

23) **«la minimizzazione»:** consiste nella raccolta dei soli dati pertinenti, quindi limitando il trattamento a ciò che è realmente necessario e indispensabile rispetto alla finalità alla quale sono destinati. La minimizzazione in realtà è da considerarsi un vero e proprio **principio fondamentale** (principio di pertinenza dei dati) che regolamenta il trattamento dei dati personali, perché nell'ordinamento europeo il trattamento deve sempre essere limitato ai soli dati strettamente necessari.

CHECK-LIST BREVE

	DOMANDA		NOTE
1	**Nella sua azienda sono presenti dipendenti/collaboratori ? Se si quanti?**	☒	*Sono presenti tre dipendenti con mansioni amministrative*
2	**Mi potrebbe indicare da quali delle seguenti aree organizzative è composta la sua azienda?**		
	Unica area organizzativa	☒	*Esite un'unica area organizzativa dedicata all'amministrazione delle attività dell'Ordine dei Medici e Chirurghi di Forlì e Cesena*
	ICT	☐	
	Risorse umane	☐	
	Area tecnica	☐	
	Commerciale e Marketing	☐	
	Area fornitori	☐	
	Amministrazione e controllo	☐	
	Altro	☐	
3	**La sua azienda tratta particolari categorie di dati personali (ex dati sensibili)?**	☒	*Sono conservati i dati necessari alla gestione del personale. Inoltre possono essere conservati anche dati relativi a condanne penali e reati di eventuali appartenenti all'Ordine. Questo per poter definire eventuali sospensioni o espulsioni di medici dall'Ordine a seguito di comportamenti non eticamente corretti.*
	Se si, quali tra quelli indicati?		
	Dati che rivelano l'origine razziale o etnica	☐	*Sono conservati i dati relativi a condanne e reati di iscritti all'Ordine. Questi vengono utilizzati per valutare il comportamento dell'iscritto nello svolgimento della professione medica e per poter definire sospensioni o espulsioni dall'Ordine stesso.*
	Dati che rilevano le opinioni politiche	☐	
	Dati che rivelano le condizioni religiose o filosofiche	☐	
	Dati che rivelano l'appartenenza sindacale	☐	
	Dati genetici	☐	
	Dati biometrici	☐	
	Dati relativi alla salute	☐	
	Dati relativi alla vita/orientamento sessuale	☐	
	Dati relativi a condanne penali e reati	☒	
4	**Uno o più trattamenti possono considerarsi effettuati su larga scala?**	☐	

	Se si, mi può indicare quale/i?		
5	**Nella sua azienda il trattamento dei dati avviene per specifiche finalità. Ci potrebbe indicare quali?**		
	Adempimento obblighi contrattuali	☐	*Adempimento dei Compiti e delle funzioni assegnate per legge all'Ordine dei Medici.*
	Adempimento obblighi di legge	☒	
	Marketing diretto	☐	
	Marketing indiretto	☐	
	Elaborazione statistiche (anonime) interne	☐	
	Gestione rapporti di lavoro	☐	
	Tutela del patrimonio azienale	☐	
	Sicurezza degli ambienti di lavoro	☐	
	Gestione clienti	☐	
	Gestione fornitori	☒	
	Gestione del contenzioso	☒	
	Altro	☒	
6	**Ci potrebbe indicare quali sono le categorie di destinatari dei dati?**		
	Titolare/Responsabile	☒	*Chiunque voglia consultare l'Albo degli appartenenti all'Ordine dei Medici, avendo quest'ultimo il compito, per statuo, di rendere di pubblico accesso l'elenco dei medici iscritti.*
	Collaboratore familiare del titolare/responsabile	☐	
	Consulente professionale	☒	
	Dipendente/collaboratore	☒	
	Fornitori	☐	
	Partner	☐	
	Pubbliche autorità e amministrazioni	☒	
	Banche e istituti finanziari	☒	
	Società esterne per obblighi amministrativi, contabili e gestionali	☒	
	Altro	☒	
7	**La sua azienda ha individuato la base giuridica (ovvero la giustificazione legale) per cui i dati possono essere trattati?**		
	Consenso	☒	*L'Ordine ha per legge il dovere di aggiornare l'elenco degli iscritti all'Albo e di rendere pubblici e*
	Obbligo contrattuale	☐	
	Obbligo legale	☒	

	Interesse vitale	☐	*disponibili alle autorità e ai cittadini tali elenchi.*
	Interesse legittimo del titolare	☐	
	Interesse pubblico	☒	
8	**La sua azienda ha individuato il periodo massimo entro il qulae i dati possono essere trattati o conservati?**		
	Scadenza rapporto contrattuale	☐	
	Scadenza del termine di durata obblighi legali	☒	
	Venir meno dell'interesse legittimo del titolare	☐	
	Venir meno dell'intersse pubblico	☒	
	Altro criterio	☐	
9	**Mi potrebbe indicare quali assets sono utilizzati in azienda?**		
	Archivio cartaceo	☒	
	Automezzo	☐	
	Cellulari	☐	
	Database	☒	
	Desktop	☒	
	Dispositivi di backup	☒	
	Dispositivi di localizzazione	☐	
	Dispositivi di rilevamento biometrico	☐	
	Dispositivi di sorveglianza	☐	
	Notebook	☐	
	Posta elettronica	☒	
	Risorsa umana	☐	
	Server	☒	
	Server in cloud	☐	
	Sito internet	☐	
	Social media	☐	
	Software	☒	
	Tablet	☐	
	Altro	☐	
10	**I dati vengono trasferiti o archiviati in un Paese extra-UE?**	☐	

CHECK_LIST MISURE TECNICO-ORGANIZZATIVE

A	*DATI, INFORMATIVE, CONSENSO, NOMINE, DIRITTI DELL'INTERESSATO, CODICE DI CONDOTTA, CERTIFICAZIONE*		
1	**Ha stabilito i tempi di conservazione dei dati? Cancello le informazioni di cui non ho più bisogno?**	☒	*L'ordine ha stabilito i tempi di conservazione ma devono ancora essere definite le modalità tecniche di cancellazione dei dati nei software gestionali utilizzati dall'Ordine.*
2	**L'accesso ai dati personali è limitato alle sole persone che hanno necessità di averne conoscenza?**	☒	*INCARICATI INTERNI E RESPONSABILI ESTERNI.*
3	**E' stata fornita l'informativa a dipendenti/collaboratori, clienti, fornitori ed altri interessati (es. utilizzatori sito web)?**	☒	*INFORMATIVA POSTA ELETTRONICA - INFORMATIVA DIPENDENTI IN FORZA CON CONSENSO*
4	**Le informative sono personalizzate sulla base delle tipologie di trattamento effettuati, delle finalità e dei soggetti coinvolti?**	☒	
5	**È presente l'informativa nei moduli fax, nelle e-mail e sul sito internet?**	☒	*INFORMATIVA POSTA ELETTRONICA*
6	**In caso di dati sensibili, si dispone del consenso esplicito o si tratta di assolvimento di obblighi o esercizio di diritti in materia di rapporto di lavoro?**	☒	*I dati sensibili possono riguardare controversie fra sanitario e sanitario, o fra sanitario e persona, od enti a favore dei quali il sanitario abbia prestato o presti la propria opera professionale. L'Ordine dei Medici in caso di controversie ha l'obbligo di intervenire per valutare se i comportamenti sono stati deontologicamente corretti.*
7	**Se, al di fuori dell'impresa (es. outsourcing), enti o persone fisiche trattano dati personali nel suo interesse, sono stati designati quali responsabili del trattamento?**	☒	*Sono stati designati con nomina formale tutti gli enti e persone fisiche che vengono in contatto dei dati in possesso dell'Ordine dei Medici.* .
	Se si, potrebbe fornire i dati di contatto (nome, telefono ed email)?		*Tutti i contatti sono elencati nell'organigramma allegato al Registro dei Trattamenti*
8	**La designazione del/i responsabile/i del trattamento è avvenuta in maniera formale (es. contratto, etc.)?**	☒	*Una copia delle lettere di nomina sono conservate presso l'Ordine.*

9	**E' stato designato un Data Protection Officer (DPO)? Potrebbe fornire i dati di contatto (nome, telefono ed email)?**	☒	*DPO: Gaspari Luca cell. 3283105961 email: lgaspari@pec.it*
10	**All'interno dell'azienda, sono stati individuati gli incaricati del trattamento?**	☒	*Sono stati nominati con atto formale tutti i dipendenti e tutti i componenti del Consiglio Direttivo, della Commisione Medica, del Collegio dei Revisori dei Conti e della Commissione Albo Odontoiatri.*
B	***FORMAZIONE***		
1	**Il personale è stato informato sul fatto di non lasciare i dispositivi informatici (pc, smartphone, tablet, etc.) incustoditi o accessibili durante la loro assenza?**	☒	*ISTRUZIONI AGLI INCARICATI REGOLAMENTO INTERNO*
2	**È effettuata la formazione iniziale e periodica ai dipendenti e ai collaboratori?**	☒	*Si è tenuto un incontro all'Ordine in cui sono state affrontate le problematiche principali inerenti la gestione delle procedure Privacy. E' stato consegnato del materiale informativo che illustra il nuovo regolamento europeo GDPR nei suoi aspetti principali. E' previsto un audit annuale*
3	**Titolare e (se presente) responsabile/i del trattamento partecipano alla formazione periodica?**	☒	
4	**Sono state fornite al dipendente/collaboratore norme sull'uso dei dispoitivi aziendali e su quello dei dispositivi personali?**	☒	
5	**Le suddette norme sono contenute in un documento aziendale reso disponibile al dipendente/collaboratore (regolamento aziendale)?**	☒	*E' stato distribuito un regolamneto interno.*
C	***SICUREZZA FISICA***		
1	**Sono presenti estintori vicino al PC/server?**	☒	
2	**Le porte degli uffici sono chiuse (a chiave per i dati sensibili) nei momenti di pausa, assenza)?**	☒	*Gli uffici risultano presidiati da almeno un collega e in caso di assenza non risultano accessibili al pubblico.*

3	**E' presente un sistema di videosorveglianza?**	☐	*Non è presente*
	Se si, viene rispettato il provvedimento Generale del Garante?	☐	
	Le videocamere sono piazzate e puntate nel modo giusto, in modo da non violare la privacy di nessuno?	☐	
	I dati della videosorveglianza sono adeguatamente protetti?	☐	
	Come e chi ha accesso ai dati della videosorveglianza?		
	E' prevista l'informativa ridotta e completa (cartello videosorveglianza)?	☐	
D	***SICUREZZA CARTACEA***		
1	**Gli incaricati evitano che le persone non autorizzate accedano ai documenti contenenti dati sensibili? Se non più in uso dagli autorizzati, tali documenti sono riconsegnati o archiviati al termine del trattamento?**	☒	*I documenti non più in uso vengono archiviati*
2	**Le scrivanie degli uffici sono sgrombre da documenti contenenti dati personali non strettamente correlati all'attività quotidiana/settimanale?**	☒	
3	**I documenti cartacei contenenti dati personali sono archiviati in appositi contenitori e dentro gli armadi?**	☒	*Con particolare attenzione alla documentazione che contiene dati inerenti contenziosi come pure i verbali delle commissioni mediche per l'invalidità degli iscritti all'Ordine. Questi ultimi vengono poi comunicati all'Ente Previdenziale per l'erogazione della pensione. Tutti gli elenchi sullo stato vaccinale degli iscritti all'Albo vengono protocollati e conservati all'interno di armadi, in modo che siano accessibili solo al personale autorizzato.*
4	**Sono presenti armadi chiusi a chiave per la custodia dei dati sensibili (malattie, infortuni, visite mediche, buste paga, etc.)? A tali archivi accedono solo le persone autorizzate?**	☒	*Particolare attenzione viene riposta alla documentazione che contiene dati inerenti contenziosi legali, come pure ai verbali delle commissioni mediche per l'invalidità degli iscritti all'Ordine. Questi ultimi vengono poi comunicati all'Ente Previdenziale per l'erogazione della pensione*

5	**Sono distrutte le fotocopie mal risucite contententi dati personali, rendendole del tutto illegibbili e non ricostruibili?**	☒	
6	**E' direttamente seguita dall'interessato la stampa di documenti riservati contenenti dati personali su stampanti condivise?**	☒	
E	***SICUREZZA INFORMATICA***		
1	**L'accesso ai dispositivi (pc, smartphone, tablet, etc.) è protetto da credenziali differenti per ogni utente?**	☒	*I PC aziendali sono protetti da password personali.*
2	**La password è composta da almeno 8 caratteri e da almeno 3 su 4 dei seguenti gruppi di caratteri: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (simboli)?**	☒	
3	**Gli incaricati possono scambiarsi fra loro username e password o sono utilizzati post it per ricordare la password?**	☐	
4	**I profili non utilizzati o in caso di perdita delle qualità dell'incaricato sono correttamente disattivati?**	☒	
5	**E' disciplinando l'uso di internet e della strumentazione elettronica?**	☒	*E' stato distribuito un regolamento interno che disciplina l'utilizzo di internet e delle apparecchiature elettroniche.*
6	**Si eseguono controlli e/o monitoraggi sulla strumentazione o le comunicazioni elettroniche (ad esempio: monitoro le email dei miei dipendenti)?**	☐	*Non vengono eseguiti monitoraggi*
	Se si, sono certo di poterlo fare? So in che limiti posso monitorare le email? Ho informato i dipendenti di questa attività, gli ho spiegato in quali circostanze avviene o perché? Sono sicuro di non violare lo Statuto dei lavoratori o la segretezza della corrispondenza?		
7	**Se ho bisogno di diffondere i dati personali di qualcuno sul web (website, social, ecc.), compresi quelli dei miei dipendenti, gli do le necessarie informazioni? Raccolgo i consensi?**	☐	*L'Ordine pubblica sul proprio sito l'elenco dei medici iscritti all'Albo dovendo in primo luogo garantire a tutti i cittadini la possibilità di verificare l´effettiva iscrizione di un medico o di un odontoiatra e, dunque, il possesso dei titoli e delle*

			competenze indispensabili per esercitare la professione.
8	**Il personale dipendente è stato formato relativamente all'utilizzo sui social di profili aziendali?**	☐	*Non vengono utilizzati profili social riconducibili all'Ordine*
9	**Con particolare riferimento al cloud computing, si è considerato che la riservatezza e la disponibilità delle informazioni allocate dipendono da: i meccanismi di sicurezza adottati dal service provider, dalla qualità della connettività di rete, dalla normativa (anche relativa agli eventali contenziosi) del paese ospitante il fornitore di servizi in cloud, dall'adozione da parte del fornitore di servizi di tecnologie proprietarie che potrebbero rendere complessa o negare la transizione di dati da un sistema cloud ad un altro**		*I servizi in cloud utilizzati dell'Ordine sono quelli relative alla gestione dell'iscrizione all'Albo provinciale e nazionale. Questo servizio è fornito in CLOUD da TECSIS.Mentre la gestione contabile e del protocollo è fatta su un server local. E sono servizi erogati all'interno della comunità europea.*
10	**E' previsto l'obbligo da parte del dipendente o del collaboratore di informare l'azienda in caso di smarrimento di un dispositivo elettronico?**	☐	*I dipendenti non utilizzano dispositivi elettronici aziendali al di fuori dell'azienda stessa*
11	**E' prevista la pseudonomizzazione dei dati personali?**	☐	
12	**Nel caso in cui il dipendente o il collaboratore sia dotato di un dispositivo elettronico aziendale e questo non sia crittografato, è prevista la possibilità - in caso di smarrimento o furto - di cancellare anche a distanza i dati?**	☐	*Non sono presenti dispositivi elettronici in dotazione ai dipendenti al di fuori degli uffici dell'Ordine.*
13	**E' previsto un audit privacy periodico?**	☒	*E' previsto un Audit con cadenza annuale.*
14	**E' prevista una gestione dei log che permetta di ricostruire chi e quando ha effettuato un accesso o un operazione di lettura, creazione, aggiornamento, eliminazione di un dato personale**	☐	
15	**I dati personali (e soprattutto quelli 'particolari', ex sensibili) quando non più utilizzati su base giornaliera, ma che non hanno ancora raggiunto la durata massima di conservazione prevista, vengono archiviati separatamente in maniera sicura?**	☒	
16	**E' attiva una rete wifi che consente di collegare il terminale agli altri?**	☒	*La rete wifi presente in ufficio è una linea dati separata dalla rete dati*

			aziendale, e viene utilizzata dagli ospiti che in questo modo non condividono nessun dato con la rete interna, Il WIFI è comunque protetto da password, ma non è stato definito un responsabile.
	Se si, è protetta adeguatamente da una password e se si, chi ne è a conoscenza?	☒	
	L'accesso a tale rete è limitato a terminali specifici o no?	☒	
17	**Le cartelle condivise presenti sulla rete sono protette adeguatamente da accessi indesiderati?**	☒	
F	***SOFTWARE, ANTIVIRUS, FIREWALL***		
1	**Sono presenti sistemi di blocco per smartphone e tablet?**	☐	*Non sono presenti smartphone e tablet dell'Ordine*
2	**Sono attivi sistemi per il blocco del terminale in caso di inattività prolungata dell'utente sullo stesso?**	☒	
3	**Sul terminale è attivo l'antivirus ed è regolarmente aggiornato?**	☒	*E' presente un sitema antivirus installato su tutti i PC della rete aziendale.*
4	**Il sistema operativo in uso gode ancora del supporto ufficiale con relativo rilascio degli aggiornamenti di sicurezza?**	☒	
5	**Firewall hardware e/o software sono regolarmente aggiornati?**	☒	
G	***BACK-UP, LEGGIBILITA', RIPRSTINO***		
1	**È effettuato il back up di tutti i dati (sia su server, sia su client) almeno settimanalmente su supporto esterno (cartuccia/cassetta, NAS, HDD-USB, etc.) in base ad un predefinita procedura?**	☒	*Il backup dei dati aziendali è garantito dall fornitore delle procedure per I software in Cloud (Tecsis). Mentre per I software in locale è previsto un Backup giornaliero su NAS.*
2	**I supporti di back up sono custoditi in luogo separato dai PC/server e protetti da incendio e furto ed accessibili solo al responsabile della custodia ed archiviazione?**	☒	*I backup sono custoditi in una stanza accessibile solo con l'intervento del personale dell'ordine.*
3	**Sono individuate le figure di responsabile e di custodia dei back up?**	☒	*E' stato individuate come responsabile Gavelli Michele*
4	**Viene eseguita una verifica dell'esito del backup?**	☒	

5	**Sono effettuate prove per il ripristino dei dati su PC/server in tempi certi (al massimo 7 giorni) e compatibili con i diritti dell'interessato?**	☐	.
6	**Il back up è crittografato rendendone illeggibile il contentuo a soggetti non autorizzati?**	☐	
7	**Vengono notificati al responabile eventuali errori nella creazione del backup(ad esempio tramite email)?**	☐	
H	***TRASFERIMENTO DEI DATI IN PAESI TERZI***		
1	**Se trasferisco dati all'estero, so che c'è un divieto che può essere superato solo in alcuni casi definiti dalla legge?**	☐	
2	**So che l'uso di servizi web (cloud, email) può comportare un trasferimento dei dati all'estero?**	☐	
3	**So che il divieto di trasferimento opera anche in questi casi (il trasferimento è possibile solo se ricorrono i presupposti di legge)?**	☐	
4	**Se i dati personali trattati dall' impresa sono soggetti a trasferimento verso Paesi terzi (esterni all'Unione europea e all'area economica europea), il trasferimento avviene:**		
	in presenza di una delle condizioni previste dall'art. 43 del Codice?	☐	
	verso uno dei paesi che assicurano un livello adeguato di protezione	☐	
	Verso un'impresa statunitense che aderisce al Safe Harbor ora Privacy Shield	☐	
	in presenza di clausole contrattuali standard tra esportatore e importatore	☐	
	in presenza di un'autorizzazione ad hoc da parte del Garante	☐	

REGISTRO DEI TRATTAMENTI

Registro dei trattamenti art. 30 del Regolamento UE 2016/679

Nome Organizzazione	Ordine dei Medici Forlì e Cesena		**Data ultimo aggiornamento** 10/09/2025
Indirizzo	Viale Italia 153, Forlì		
Figura	**Nome**	**Telefono**	**E-mail**
Titolare	Ordine dei Medici Forlì e Cesena	0543 27157	info@ordinemedicifc.it
Responsabile	Dott.ssa Marcella Manuzzi	054328035	m.manuzzi@studio-manuzzi.com
Responsabile	Studio dott.ssa Marilena Valgiusti	0543795631	paghe@studiovalgiusti.it
Responsabile	Tecsis srl	0497309333	info@tecsis.it
Responsabile	Ing. Sara Palai	3286647877	sarapalai@libero.it
Responsabile	Avv. Francesco Farolfi	0543 34746	
Responsabile	FNOMCeO	06362031	info@fnomceo.it
Responsabile	Allianz Ras Mosconi-Pierotti-Pratesi SRL	0543404101	agenzia@mppassicurazioni.com

Titolo trattamento	Gestione Contenziosi
Area	**Unica area organizzativa**
Data Inserimento	06/11/2018
Data Modifica	10/09/2025
Termine	Obblighi di legge
Titolare	Ordine dei Medici Forlì e Cesena
Responsabile	Avv. Francesco Farolfi
Note	
Tipologie	Dati personali Dati relativi a condanne penali e reati
Finalita	Adempimento obblighi di legge
Interessati	Altro
Destinatari	Titolare/Responsabile Consulente professionale Pubbliche autorità e amministrazioni
Misure	Misure di sicurezza fisica Misure di sicurezza cartacea Misure di sicurezza informatica Software, antivirus, firewall Back-up, leggibilità, ripristino
Asset	Archivio cartaceo
Base giuridica	Obbligo contrattuale Obbligo legale

Titolo trattamento	Ordinaria Gestione Contabile e Amministrativa
Area	Unica area
Data Inserimento	11/06/2018
Data Modifica	10/09/2025
Termine	Obblighi di legge
Titolare	Ordine dei Medici Forlì e Cesena
Responsabile	Dott.ssa Marcella Manuzzi
Note	
Tipologie	Dati Clienti e Fornitori
Finalita	Adempimento obblighi contrattuali Adempimento obblighi di legge
Interessati	Altro
Destinatari	Titolare/Responsabile Dipendente/collaboratore
Misure	Informative, consenso, nomine Formazione Misure di sicurezza fisica Misure di sicurezza cartacea Misure di sicurezza informatica Software, antivirus, firewall Back-up, leggibilità, ripristino
Asset	Archivio cartaceo Database Desktop Dispositivi di backup Server Software
Base giuridica	Obbligo contrattuale Obbligo legale

Titolo trattamento	Disbrigo di pratiche e adempimenti necessari per la gestione del rapporto di lavoro
Area	Unica area organizzativa
Data Inserimento	11/06/2018
Data Modifica	10/09/2025
Termine	Obblighi di legge
Titolare	Ordine dei Medici Forlì e Cesena
Responsabile	Studio Valgiusti Marilena
Note	
Tipologie	Dati personali Dati relativi alla salute
Finalita	Adempimento obblighi contrattuali Adempimento obblighi di legge Gestione rapporti di lavoro
Interessati	Dipendenti
Destinatari	Titolare/Responsabile Consulente professionale Dipendente/collaboratore
Misure	Informative, consenso, nomine Formazione Misure di sicurezza fisica Misure di sicurezza cartacea Misure di sicurezza informatica Software, antivirus, firewall Back-up, leggibilità, ripristino
Asset	Archivio cartaceo Database Desktop Dispositivi di backup Notebook Server Software
Base giuridica	Obbligo contrattuale Obbligo legale

Titolo trattamento	Trattamento dati relativi al D.lgs. 81/2008 sulla sicurezza e salute dei lavoratori nei luoghi di lavoro
Area	Unica area organizzativa
Data Inserimento	11/06/2018
Data Modifica	10/09/2025
Termine	Obblighi di legge
Titolare	Ordine dei Medici Forlì e Cesena
Responsabile	Ing. Sara Palai
Note	
Tipologie	Dati personali Dati relativi alla salute
Finalita	Adempimento obblighi contrattuali Adempimento obblighi di legge Gestione rapporti di lavoro
Interessati	Dipendenti
Destinatari	Titolare/Responsabile Consulente professionale Dipendente/collaboratore
Misure	Informative, consenso, nomine Formazione Misure di sicurezza fisica Misure di sicurezza cartacea Misure di sicurezza informatica Software, antivirus, firewall Back-up, leggibilità, ripristino
Asset	Archivio cartaceo Database Desktop Dispositivi di backup Notebook Server Software
Base giuridica	Obbligo contrattuale Obbligo legale

Titolo trattamento	Controllo iscritti Albo
Area	Unica area organizzativa
Data Inserimento	22/12/2021
Data Modifica	10/09/2025
Termine	Obblighi di legge
Titolare	Ordine dei Medici Forlì e Cesena
Responsabile	FNOMCeO
Note	Vengono inviati elenchi degli iscritti all'Albo
Tipologie	Dati personali
Finalita	Adempimento obblighi di legge
Interessati	Altro
Destinatari	Titolare/Responsabile Pubbliche autorità e amministrazioni
Misure	Informative, consenso, nomine Formazione Misure di sicurezza fisica Misure di sicurezza cartacea Misure di sicurezza informatica Software, antivirus, firewall Back-up, leggibilità, ripristino
Asset	Posta elettronica Archivio cartaceo Dispositivi di backup
Base giuridica	Obbligo legale

Titolo trattamento	Attività di gestione, manutenzione e assistenza del software in cloud
Area	Unica area organizzativa
Data Inserimento	19/06/2024
Data Modifica	10/09/2025
Termine	Obblighi di legge
Titolare	Ordine dei Medici Forlì e Cesena
Responsabile	Tecsis srl
Note	
Tipologie	Dati personali Dati relativi alla salute
Finalita	Fornire servizi di hosting e manutenzione del software Assistenza tecnica Altre attività di supporto e consulenza definite nel contratto di servizio,
Interessati	Clienti Fornitori
Destinatari	Società esterna servizi hosting
Misure	Informative, consenso, nomine Formazione Crittografia dei dati a riposo e/o in transito (se applicabile); Sistemi di autenticazione e autorizzazione con credenziali protette; Sistemi di monitoraggio e logging degli accessi; Backup periodici, soluzioni di disaster recovery e business continuity; Firewall, antivirus e protezioni contro attacchi informatici; Procedure di controllo degli accessi fisici ai data center (se rilevante).
Asset	Database Servizi in Cloud Dispositivi di backup Software
Base giuridica	Obbligo contrattuale Obbligo legale

Titolo trattamento	Attività di gestione assicurazione consiglieri Ordine
Area	Unica area organizzativa
Data Inserimento	11/06/2018
Data Modifica	10/09/2025
Termine	Obblighi di legge
Titolare	Ordine dei Medici Forlì e Cesena
Responsabile	Allianz Ras Mosconi-Pierotti-Pratesi SRL
Note	
Tipologie	Dati personali
Finalita	Adempimento contratti assicurativi
Interessati	Consiglieri Ordine Medici
Destinatari	Società esterne per obblighi amministrativi, contabili e gestionali
Misure	Informative, consenso, nomine
Asset	Archivio cartaceo Email
Base giuridica	Obbligo legale

Glossario:

- "***Data inserimento***": la data di creazione del registro.
- "***Data modifica***": la data ultima in cui il registro è stato modificato.
- "***Termine***": il periodo massimo entro il quale i dati oggetto del trattamento vengono trattati e/o conservati dal titolare. La normativa europea in materia di Privacy prevede che i dati debbano essere conservati per un periodo di tempo limitato, e in particolare non oltre il tempo necessario per raggiungere lo scopo alla base del trattamento. Nel caso in cui un titolare del trattamento volesse mantenerli per un periodo superiore, deve procedere alla loro anonimizzazione.
- "***Tipologie di dati***", quali**:
  - *dati personali,* ricoducibili a qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. «*interessato*»)*;
  - *dati che rivelano l'origine razziale o etnica,* ovvero quei dati che forniscono informazioni specifiche relativamente all'appartenenza ad etnie o minoranze culturali*;*
  - *dati che rivelano le opinioni politiche;*
  - *dati che rivelano le condizioni religiose o filosofiche;*
  - *dati che rivelano l'appartenenza sindacale*, quali, ad esempio, l'essere iscritto ad un sindacato, come si desume dalla trattenuta sulla busta paga;
  - *dati genetici,* ovvero quei 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**;
  - *dati biometrici,* nonché 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*;
  - *dati relativi alla salute,* ossiai 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**;*
  - *dati relativi alla vita o all'orientamento sessuale;*
  - *dati relativi a condanne penali e reati*, ovvero i dati cc.dd. "*giudiziari*", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679(articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.
- "***Interessati"***: le persona fisiche (comprese le ditte individuali per la normativa italiana) delle quali vengono trattati dati personali e categorie particolari di dati personali.
- "***Misure"***:tutto ciò che viene posto in essere dal titolare per proteggere ed utilizzare in maniera adeguata e lecita i dati personali e le categorie particolari di dati personali. Tali misure sono altresì volte alla dimostrazione della conformità delle attività di trattamento, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità dello stesso, nonché del rischio per i diritti e le libertà delle persone fisiche.
- "***Assets"***: gli strumenti in cui risiedono fisicamente i dati personali.

---

*Come da Reg. 679/2016 UE.

** "Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali."

ORGANIGRAMMA

Nome Organizzazione	Ordine dei Medici e Chirurghi e Degli odontoiatri della Provincia di Forlì e Cesena	Data Creazione 16/03/2018
		Data ultimo aggiornamento 10/09/2025
Indirizzo	Viale Italia 153 – scala A 47122 Forlì (FC)	

Figura	Nome	Telefono	E-mail
Titolare Componente consiglio direttivo con incarico di Presidente e Presidente della Commissione Medica	Dott.Gaudio Michele	0543 27157	presidente@ordinemedicifc.it
Data Protection Officer	Sig. Gaspari Luca	0543452823 3283105961	gaspari@confartigianato.fo.it lgaspari@pec.it
Incaricato Add. segreteria	Sig.ra Leonelli Eliabetta	0543 27157	info@ordinemedicifc.it
Incaricato Add. segreteria	Sig.ra Laghi Laila	0543 27157	info@ordinemedicifc.it
Incaricato add.segreteria	Sig. Gavelli Michele	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Tesoriere e componente della Commissione Medica	Dott. Balistrieri Fabio	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Vice presidente e componente della Commissione Medica	Dott. Pascucci Gian Galeazzo	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Segretario	Dott. Pignatosi Francesco	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	Dott.ssa Amadei Enrico Maria	0543 27157	info@ordinemedicifc.it v

Incaricato Componente consiglio direttivo e componente della Commissione Medica con incarico di Consigliere	Dott.ssa Cangialeoni Sara	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	Dott. Castellini Angelo	0543 27157	info@ordinemedicifc.it
Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	Dott. Ceccaroni Luigi	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere	Dott.ssa De Cesare Simona	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	Dott. Ercolani Giorgio	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	Dott. Ludovico Cosimo	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	Dott. Macacchi Massimiliano	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	Dott.ssa Musacchia Giorgia	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e	**Dott.Paganelli Paolo**	0543 27157	info@ordinemedicifc.it

incarico Presidente della Commissione Albo Odontoiatri			
Incaricato Componente consiglio direttivo con incarico di Consigliere e incarico di Vice Presidente della Commissione Albo Odontoiatri	**Dott. Raspini Mario**	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Consigliere e componente della Commissione Medica	**Dott. Ragazzini Paolo**	0543 27157	info@ordinemedicifc.it
Incaricato Componente della Commissione Medica	**Dott. Pignatosi Francesco**	0543 27157	info@ordinemedicifc.it
Incaricato Componente consiglio direttivo con incarico di Componente della Commissione Albo Odontoiatri	Dott.ssa Tognali Daniela	0543 27157	info@ordinemedicifc.it
Incaricato Consigliere della Commissione Albo Odontoiatri	Dott. Alberti Andrea	0543 27157	info@ordinemedicifc.it
Incaricato Consigliere della Commissione Albo Odontoiatri	Dott. D'Arcangelo Domenico	0543 27157	info@ordinemedicifc.it
Incaricato Consigliere Comm. Odontoiatri	Dott. Zanetti Daniela	0543 27157	info@ordinemedicifc.it
Incaricato Presidente del collegio dei revisori dei conti	Dott.ssa Rossi Barbara	3382572802	mailto:dot.barbararossi@virgilio.it
Incaricato componente collegio dei Revisori dei Conti	Dott. Fabbroni Giovanni	0543 27157	info@ordinemedicifc.it
Incaricato componente collegio dei Revisori dei Conti	Dott.ssa Possanzini Paola	0543 27157	info@ordinemedicifc.it
Incaricato componente supplente collegio dei Revisori dei Conti	Dott. Seconi Marco	0543 27157	info@ordinemedicifc.it
Responsabile prevenzione della Corruzione e della	Dott. Ceccaroni Luigi	0543 27157	info@ordinemedicifc.it

Trasparenza e referente segnalazioni Whistleblowing			
Responsabile arbitro in caso di Controversie	Avv. Francesco Farolfi	0543 34746	Viale Giacomo Matteotti 115 47122 Forlì (FC)
Responsabile consulente del lavoro	Studio Valgiusti Marilena	0543 795631	Via Talete 4 47122 Forlì (FC)
Responsabile consulente informatico	Tecsis srl	049 730 9333	Viale Svezia, 16, 35020 Ponte San Nicolò PD
Responsabile Amministratore di Sistema Esterno	Sig. Massimo Amoruso	049 730 9333	Viale Svezia, 16, 35020 Ponte San Nicolò PD
Responsabile Consulente fiscale	Dott.ssa Manuzzi Marcella	0543 28035	Via Guido Bonali 1 – Forlì (FC)
Responsabile Sicurezza nei luoghi di Lavoro	Ing. Sara Palai		Via Alberi 16F 47121 Forlì (FC)

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)
in base alle previsioni del Regolamento (UE) 2016/679

-COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?*

Una 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.
Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.
Alcuni possibili esempi:
- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

-COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.
Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.
Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere **accompagnate dai motivi del ritardo.**
Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.
Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali, ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

-CHE TIPO DI VIOLAZIONI DI DATI PERSONALI VANNO NOTIFICATE?

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.
Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

-COME INVIARE LA NOTIFICA AL GARANTE?

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/ (VEDI: Provvedimento del 27 maggio 2021).

ATTENZIONE

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante. Il facsimile è allegato anche a questo documento a partire dalla pagina seguente.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

-LE AZIONI DEL GARANTE

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

** La scheda ha mero valore divulgativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento (UE) 2016/679.*

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

Questo servizio *online* per la notifica di una violazione dei dati personali deve essere utilizzato esclusivamente da soggetti (pubbliche amministrazioni, imprese, associazioni, partiti, professionisti, ecc.) che trattano dati personali in qualità di titolari del trattamento.

Per rivolgersi al Garante in qualità di interessato, per lamentare una violazione della disciplina in materia di protezione dei dati personali, occorre inviare una segnalazione (art. 144 del Codice in materia di protezione dei dati personali) che il Garante può valutare anche ai fini dell'emanazione di provvedimenti correttivi, oppure proporre un reclamo (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-*bis* a 143 del Codice in materia di protezione dei dati personali).

Maggiori informazioni sono disponibili sul sito istituzionale del Garante (https://www.gpdp.it/web/guest/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali).

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Notifica di una violazione dei dati personali

art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del D.Lgs. 51/2018

A) Dati del soggetto che effettua la notifica

Il soggetto che effettua la notifica è la persona fisica che, per conto titolare del trattamento, tramite questa procedura *online* notifica una violazione dei dati personali al Garante, assumendosi la responsabilità circa la veridicità delle informazioni fornite. Pertanto, la notifica dovrà essere effettuata dal rappresentante legale del titolare del trattamento o da un altro soggetto che agisce su sua delega.

Il sottoscritto Cognome[1*] ……. Nome[1*] …….
E-mail[2*]
…… nella
sua qualità[3] di

- ○ rappresentante legale
- ○ delegato del rappresentante legale

  Cognome[4*] ……. Nome[4*] …….

notifica la seguente violazione di dati personali e ☐ dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*) o dell'art. 44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato.

---

[1] Indicare il **Cognome** e il **Nome** del soggetto che effettua la notifica (e che successivamente dovrà apporre la sua firma digitale, conformemente alle istruzioni che riceverà via e-mail).

[2] Indicare un indirizzo **E-mail** valido per la ricezione delle istruzioni per il completamento della procedura di notifica. Nel caso venga indicata una casella PEC, verificare che la stessa sia abilitata alla ricezione di messaggi di posta elettronica ordinaria. Si consiglia, inoltre, di verificare che il messaggio non sia stato spostato automaticamente o per errore nella cartella "spam" o "posta indesiderata.

[3] Indicare se il soggetto che effettua la notifica è il "rappresentante legale" del Titolare del trattamento dati – di cui alla successiva Sez. C - oppure se agisce in **qualità** di "delegato del rappresentante legale.

[4] Qualora la notifica venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante (il rappresentante legale).

B) Tipo di notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore (**Prima notifica**). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (**Notifica integrativa**) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

- ***Prima notifica***
  - a) Completa
  - b) Preliminare[1]

  La notifica viene effettuata
  - ai sensi dell'art. 33 del RGPD
  - ai sensi dell'art. 26 d.lgs. 51/2018
- ***Notifica integrativa***[2]
  - c) fascicolo n.[3*] …… PIN [3*] ……

[1] Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa per completare il processo di notifica.

[2] Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento, integra una precedente notifica.

[3] È necessario inserire il numero del fascicolo ed il relativo PIN. Il numero di **fascicolo** unitamente al PIN sono indicati nella e-mail, indirizzata al soggetto che ha effettuato la prima notifica, con la quale è stata comunicata la corretta conclusione della procedura.

B1) Motivo dell'integrazione

Se procedi con la notifica integrativa per i motivi a) o b) troverai le informazioni che hai già fornito con l'ultima notifica e che potrai modificare. Il suo contenuto, previa integrazione o modifica, annulla e sostituisce la precedente.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioni che hai già fornito, e non sarà possibile compilare la sez. C e i punti 2 e 3 della sez. F. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

1. Si procede all'integrazione per:

- ○ a) Fornire ulteriori informazioni senza completare il processo di notifica
- ○ b) Fornire ulteriori informazioni e completare il processo di notifica
- ○ c) Completare il processo di notifica senza fornire ulteriori informazioni
- ○ d) Annullare una precedente notifica per le seguenti motivazioni:

C) Titolare del trattamento

1. Il titolare del trattamento è:

Indicare l'eventuale registro all'interno del quale è censito il Titolare/Responsabile del trattamento che effettua la comunicazione. A tal fine si rappresenta che (cfr. DL 19 ottobre 2012, n. 179) tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad Ordini o Collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INIPEC). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

- ○ Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
  (INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)
- ○ Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi - *(Tipologie Enti: Pubbliche Amministrazioni)*
  (*IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005*)
- ○ Non censito in nessuno dei due precedenti indici

2. Dati del titolare del trattamento

Indicare le informazioni relative al Titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione*……
Codice Fiscale[1*] …… Soggetto privo di C.F./P.IVA italiana ☐
Stato*……
Provincia*……Comune* …… CAP*……
Indirizzo*……
Telefono* ……
E-mail[2]……..……
PEC[2*]……

---

[1] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;
- Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

[2] Per i soggetti che risultano essere censiti in uno degli indici INI-PEC o IPA è **obbligatorio** fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

C1) Rappresentante del titolare del trattamento non stabilito nello Spazio Economico Europeo

Il titolare del trattamento non stabilito nello Spazio Economico Europeo, qualora offra beni o servizi a interessati nello Spazio Economico Europeo, oppure effettui il monitoraggio del loro comportamento (cfr. art. 3, par. 2, del Regolamento), è tenuto, ai sensi dell'art. 27 del Regolamento, a designare per iscritto un rappresentante in uno dei Paesi dello Spazio Economico Europeo in cui si trovano i predetti interessati, fatti salvi i casi in cui il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati o dati relativi a condanne penali e reati, ed è improbabile che presenti un rischio per i diritti e le libertà degli interessati, oppure il trattamento è effettuato da autorità o organismi pubblici.

1. Rappresentante del titolare del trattamento

- ○ a) Compila la sezione
- ○ b) Procedi con la notifica senza compilare questa sezione

2. Dati del rappresentante del titolare del trattamento

Denominazione[1*] ……
Codice Fiscale/P.IVA* …… Soggetto privo di C.F./P.IVA italiana ☐
Stato* ……
Provincia* …… Comune* …… CAP*
…… Indirizzo*
……
… Telefono* ……
E-mail[2*]
……
…… PEC[2*]
……
……

---

[1] Indicare le informazioni relative al Rappresentante del titolare del trattamento (nel caso di impresa indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).
[2] È obbligatorio fornire almeno un recapito tra E-mail e PEC.

D) Dati di contatto per informazioni relative alla violazione

Il titolare del trattamento deve comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni (cfr. art. 33, par. 3, lett. b), del Regolamento).

- ***1) Responsabile della protezione dei dati***
  - i cui dati di contatto sono stati già comunicati con la comunicazione protocollo[1*] n.…….
  - i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone[2] del numero di protocollo della relativa comunicazione

    Cognome* ……. Nome*

    ……. E-mail* …….

    Recapito telefonico per eventuali comunicazioni* ……..……

- ***2) Altro soggetto***

  Cognome* ……. Nome*

  ……. E-mail* …….

  Recapito telefonico per eventuali comunicazioni* ……..…… Funzione rivestita* ……..…….

---

[1]Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

[2] Selezionare questa opzione se al momento della compilazione non è possibile reperire il numero di protocollo assegnato alla comunicazione dei dati di contatto che sarà comunicato con una successiva notifica integrativa.

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile[1])

Denominazione[2*]……..……..…….
Codice Fiscale[3*] ……..……..…Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

Denominazione[2*] ……
Codice Fiscale[3*] ……..……..…Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

Denominazione[2*] ……
Codice Fiscale[3*] ……..……..…Soggetto privo di C.F./P.IVA ☐
Ruolo O Contitolare O Responsabile

---

[1] In tale tipologia rientra anche l'altro responsabile (c.d. sub-responsabile) di cui all'art. 28, par. 2, del RGPD o all'art. 18, comma 2, del d.lgs. 51/2018.

[2] Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

[3] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;

Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

F) Informazioni sulla violazione

1. *Momento in cui è avvenuta la violazione*

- a) Il _____ /_____ /_____
- b) Dal _____/_____ /_____ (la violazione è ancora in corso)
- c) Dal _____/_____ /_____ al _____ /_____ /_____
- d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. *Modalità con la quale il titolare è venuto a conoscenza della violazione*

- a) Rilevazione da parte del titolare[1]
- b) Comunicazione da parte del responsabile del trattamento
- c) Segnalazione da parte di un interessato
- d) Segnalazione da parte di un soggetto esterno
- e) Notizie stampa
- f) Altro

3. *Momento in cui il titolare è venuto a conoscenza della violazione*

Data …….. **Ora** ……..

4. *Motivi del ritardo (in caso di notifica oltre le 72 ore)*

5. *Natura della violazione*

[ ] a) Perdita di riservatezza[2] [ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. *Causa della violazione*

[ ] a) Azione intenzionale interna

[ ] b) Azione accidentale interna

[ ] c) Azione intenzionale esterna

[ ] d) Azione accidentale esterna

[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. *Descrizione della violazione*[5]

8. *Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione*

9. *Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti*

10. Categorie di interessati coinvolti nella violazione

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali) [ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali [ ] e) Beneficiari o assistiti
[ ] f) Pazienti [ ]
g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- a) N.....interessati
- b) Circa n.....interessati
- c) Non determinabile
- d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza [ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica [ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche [ ] o) Dati che rivelano l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale [ ] q) Dati relativi alla salute
[ ] r) Dati genetici

[ ] s) Dati biometrici
[ ] t) Altro

[ ] u) Categorie ancora non determinate

13. Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione

- a) N. ……..
- b) Circa n. ……..
- c) Non determinabile
- d) Non ancora determinato

14. Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati

15. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

---

1. Es. verifiche interne, monitoraggi, ecc
2. Diffusione/ accesso non autorizzato o accidentale
3. Modifica non autorizzata o accidentale
4. Impossibilità di accesso o distruzione non autorizzata o accidentale
5. Indicare le circostanze in cui si è verificata la violazione e le cause, tecniche o organizzative, che l'hanno determinata
6. Ad esempio numero di fatture, ordini, referti, immagini, record di un database o numero di transazioni.

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

[ ] a) I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento

[ ] b) I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati

[ ] c) I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito

[ ] d) Altro

[ ] e) In corso di valutazione[4]

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti

[ ] b) I dati sono stati modificati mantenendo la consistenza [ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi

[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi [ ] c) Altro

[ ] d) In corso di valutazione[4]

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

[ ] a) Perdita del controllo dei dati personali [ ] b)
Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità [ ] e)
Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione [ ] h)
Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale [ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

- a) Trascurabile
- b) Bassa
- c) Media
- d) Alta
- e) Non ancora definita

Motivazioni

4. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

1. ***Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati***

2. ***Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future***

3. ***Allegati***

[ ] Intendo allegare un documento contenente ulteriori informazioni

1. Nella descrizione distinguere le misure adottate da quelle in corso di adozione

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categorie e numero di registrazioni di dati personali, probabili conseguenze della violazione, ecc.) di cui il titolare del trattamento dovrebbe tenere conto nella valutazione del rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati personali. Pertanto si invita il titolare del trattamento a prestare particolare attenzione nella compilazione della presente sezione, fornendo le motivazioni che lo hanno portato a ritenere che la violazione dei dati personali sia suscettibile, o meno, di presentare un rischio elevato per gli interessati.

Il Regolamento (spec. cons. nn. 75 e 76) suggerisce che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbero essere determinati in base a una valutazione oggettiva.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i seguenti fattori da considerare – a fronte di una violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

1. *Il titolare del trattamento ritiene[1] che:*

- a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

2. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

Si evidenzia che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento è tenuto, ai sensi dell'art. 34 del Regolamento, a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, a meno che sia soddisfatta una delle condizioni previste dal par. 3 del citato articolo.

1. La violazione è stata comunicata direttamente agli interessati?

- o a) Sì, è stata comunicata il _____/____/_____
- o b) No, sarà comunicata entro il _____/____/_____
- o c) No, sono tuttora in corso le dovute valutazioni
- o d) No, perché la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- o e) No e non sarà comunicata perché:

[ ] e1) il titolare ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura);
Descrivere le misure applicate

[ ] e2) il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
Descrivere le misure adottate

[ ] e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.
Descrivere la modalità tramite la quale gli interessati sono stati informati

2. Numero di interessati a cui è stata comunicata la violazione

N..... interessati

3. Canale utilizzato per la comunicazione agli interessati

[ ] a) SMS
[ ] b) Posta cartacea
[ ] c) Posta elettronica [ ] d)
Altro

4. Contenuto della comunicazione agli interessati

5. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. *La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[1]?*

O Sì O No

Indicare a quale organismo e in virtù di quale norma

2. *È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?*

O Sì O No

Note

---

1. Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

N) Informazioni relative a violazioni transfrontaliere

Un trattamento transfrontaliero (cfr. art. 4, punto 23), del Regolamento) è un trattamento che ha luogo nell'ambito di stabilimenti in più di un Paese dello Spazio Economico Europeo (di cui fanno parte gli Stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia), oppure che ha luogo nell'ambito di un unico stabilimento in un Paese dello Spazio Economico Europeo, ma che può avere impatti significativi sui diritti e sulle libertà di interessati in più di un Paese dello Spazio Economico Europeo.

1. *La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?*

- a) Sì
- b) No
- c) Sono tuttora in corso le dovute valutazioni

2. *Indicare l'autorità di controllo capofila[1]*

- a) Garante per la protezione dei dati personali
- b) Altra autorità di controllo: [Selezionare]
- c) Non si dispone di elementi per individuare l'autorità di controllo capofila

3. *Indicare i Paesi dello Spazio Economico Europeo in cui si trovano stabilimenti del titolare, specificando quelli coinvolti nella violazione, o in cui si trovano gli interessati coinvolti nella violazione*

	Stabilimenti del titolare	Stabilimenti coinvolti nella violazione	Interessati coinvolti nella violazione
Italia	[ ]	[ ]	[ ]
Austria	[ ]	[ ]	[ ]
Belgio	[ ]	[ ]	[ ]
Bulgaria	[ ]	[ ]	[ ]
Cipro	[ ]	[ ]	[ ]
Croazia	[ ]	[ ]	[ ]
Danimarca	[ ]	[ ]	[ ]
Estonia	[ ]	[ ]	[ ]
Finlandia	[ ]	[ ]	[ ]
Francia	[ ]	[ ]	[ ]
Germania	[ ]	[ ]	[ ]
Grecia	[ ]	[ ]	[ ]
Irlanda	[ ]	[ ]	[ ]
Islanda	[ ]	[ ]	[ ]
Lettonia	[ ]	[ ]	[ ]
Liechtenstein	[ ]	[ ]	[ ]
Lituania	[ ]	[ ]	[ ]

Lussemburgo	[ ]	[ ]	[ ]
Malta	[ ]	[ ]	[ ]
Norvegia	[ ]	[ ]	[ ]
Paesi Bassi	[ ]	[ ]	[ ]
Polonia	[ ]	[ ]	[ ]
Portogallo	[ ]	[ ]	[ ]
Rep. Ceca	[ ]	[ ]	[ ]
Romania	[ ]	[ ]	[ ]
Slovacchia	[ ]	[ ]	[ ]
Slovenia	[ ]	[ ]	[ ]
Spagna	[ ]	[ ]	[ ]
Svezia	[ ]	[ ]	[ ]
Ungheria	[ ]	[ ]	[ ]

4. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI) [ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information [ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA) [ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)

[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner
[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

---

1. L'autorità di controllo dello stabilimento principale in cui ha luogo il trattamento o dello stabilimento unico del titolare del trattamento

O) Informazioni relative a violazioni che riguardano trattamento effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nello Spazio Economico Europeo, effettuato da un titolare del trattamento che non è stabilito nello Spazio Economico Europeo, laddove tale trattamento riguardi: a) l'offerta di beni o la fornitura di servizi a interessati nello Spazio Economico Europeo, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dello Spazio Economico Europeo (cfr. art. 3, par. 2, del Regolamento)

1. ***La violazione riguarda un trattamento, a cui si applica il Regolamento, effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo?***

   - o a) Sì
   - o b) No

2. ***Indicare gli altri Paesi dello Spazio Economico Europeo in cui si trovano gli interessati coinvolti nella violazione***

[ ] Austria

[ ] Belgio
[ ] Bulgaria
[ ] Cipro
[ ] Croazia
[ ] Danimarca
[ ] Estonia
[ ] Finlandia
[ ] Francia
[ ] Germania
[ ] Grecia
[ ] Irlanda
[ ] Islanda
[ ] Lettonia
[ ] Liechtenstein
[ ] Lituania
[ ] Lussemburgo
[ ] Malta
[ ] Norvegia
[ ] Paesi Bassi
[ ] Polonia
[ ] Portogallo
[ ] Rep. Ceca
[ ] Romania
[ ] Slovacchia
[ ] Slovenia
[ ] Spagna

[ ] Svezia
[ ] Ungheria

3. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI) [ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information [ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA) [ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)
[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner

[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata