ACEN - Associazione Costruttori Edili Napoli
Riviera di Chiaia, 202
80121, Napoli (NA)
Codice Fiscale: 80014380630

ANCE | NAPOLI

LINEE GUIDA

Trattamento e misure di protezione per i dati personali acquisiti con portale web aziendale

2024

Sintesi documento / Il presente documento disciplina il trattamento e le misure di protezione per i dati personali acquisiti attraverso il portale web del Titolare del Trattamento e fornisce regole e procedure applicabili per in ordine alla sicurezza che il Titolare del Trattamento applicherà ai dati personali degli utenti e dei visitatori del predetto sito internet.

Redatto da:
Dott. Guglielmo Pulcini

Per conto del
Titolare del Trattamento
ACEN

Data di applicazione:
20/05/2024

Documento valido fino al:
20/05/2025

Il Legale Rappresentante
Ing. Angelo Lancellotti

Cronologia delle revisioni

Data	Revisione	Titolarità	Classificazione
20 maggio 2024	1.1.	ACEN - Associazione Costruttori Edili Napoli	Prima redazione per adeguamento del portale web acen.it

Sommario

1. Campo d'applicazione, scopo e destinatari

Il presente documento disciplina il trattamento e le misure di protezione per i dati personali acquisiti attraverso il portale web **acen.it** della ACEN - Associazione Costruttori Edili Napoli e fornisce regole e procedure applicabili per in ordine alla sicurezza che il Titolare del Trattamento applicherà ai dati personali degli utenti e dei visitatori del predetto sito internet.

Destinatari di questo documento sono il Titolare del Trattamento ed i Responsabili del Trattamento nominati in ordine alle attività di sviluppo, implementazione ed aggiornamento del portale web.

2. Documenti di Riferimento

- Il Regolamento Generale per la Protezione dei Dati Personali (Regolamento EU 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE);
- Il Decreto Legislativo 196 del 30 giugno 2003, come integrato e modificato dal Decreto Legislativo 101 del 10 agosto 2018;
- Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali n.229 del 8 maggio 2014 "Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie";
- Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali n.231 del 10 giugno 2021 - "Linee guida cookie e altri strumenti di tracciamento";
- Linee Guida sul Consenso ai sensi del Regolamento UE 2016/679, Gruppo di Lavoro Articolo 29, WP 259 rev 0.1;
- Linee Guida sul Consenso ai sensi del Regolamento UE 2016/679, European Data Protection Board, n.5 del 2020;
- Linee Guida sulla trasparenza ai sensi del Regolamento UE 2016/679, Gruppo di Lavoro Articolo 29, WP 260 rev 0.1;
- Parere sul concetto di interesse legittimo ai sensi dell'articolo 7 della direttiva 95/46/CE", Gruppo di Lavoro Articolo 29, WP 217 rev 0.1.

3. Definizioni

Le seguenti definizioni esemplificative dei termini utilizzati nel presente documento sono tratte dall'articolo 4 del Regolamento Generale sulla Protezione dei Dati dell'Unione Europea (Regolamento Europeo 679 del 2016).

3.1. Dati personali

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.

3.2. Dati personali sensibili

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. Tra tali dati personali sensibili sono compresi i dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'appartenenza sindacale della persona, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, e dati giudiziari relativi a condanne penali e reati della persona. Per connessione, con riguardo ad una specifica protezione, è estendile a tale fattispecie di dato anche i dati personali di minori d'età.

3.3. Titolare del trattamento dei dati personali

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.

3.4. Responsabile del trattamento dei dati personali

Una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del Trattamento dei dati personali.

3.5. Trattamento dei dati personali

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.

3.6. Anonimizzazione

Deidentificazione irreversibile dei dati personali in modo tale che la persona non possa essere identificata utilizzando tempi, costi e tecnologie ragionevoli da parte del Titolare del Trattamento o di qualsiasi altra persona per identificare l'interessato. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile.

3.7. Pseudoanonimizzazione

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. La pseudonimizzazione riduce, ma non elimina completamente, la possibilità di collegare il dato personale all'interessato. Poiché i dati pseudonimizzati sono comunque dati personali, il trattamento dei dati pseudonimizzati dovrebbe essere conforme ai principi del Trattamento dei Dati Personali.

3.8. 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.

3.9. Destinatari

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.

3.10. Terzi

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.

3.11. Interessato al trattamento dei dati personali

La persona fisica cui si riferiscono i dati personali oggetto di trattamento identificata o identificabile, che può essere identificata in modo diretto o indiretto facendo riferimento, ad esempio, ad informazioni come: il nome, un numero di identificazione, dati riguardanti l'ubicazione, un identificativo on-line oppure uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

3.12. 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.

3.13. Violazione dei dati personali

Qualsiasi infrazione 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.

3.14. Autorità di Controllo

L'Autorità Pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento Generale sulla Protezione dei Dati Personali. L'Autorità di Controllo monitora qualsiasi trattamento di dati locale che incide sugli interessati o che viene effettuato da un Titolare del Trattamento o un Responsabile del Trattamento all'interno dell'Unione oppure all'esterno dell'Unione in caso il loro trattamento si rivolge a interessati residenti sul proprio territorio. I suoi compiti e poteri comprendono lo svolgimento di indagini e l'applicazione di misure amministrative e sanzioni, la promozione della consapevolezza da parte del pubblico dei rischi, delle norme, della sicurezza e dei diritti in relazione al trattamento dei dati

personali, nonché l'accesso a qualsiasi sede del Titolare del Trattamento e del Responsabile del Trattamento dei Dati, compresi eventuali strumenti e mezzi per il trattamento.

3.15. Trasferimento 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 è un 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.

4. Principi del Trattamento

4.1. Principi applicabili al trattamento dei dati personali

I principi applicabili alla protezione dei dati delineano le responsabilità delle organizzazioni nella gestione dei dati personali. L'articolo 5, comma 2, del Regolamento Generale sulla Protezione dei Dati dell'Unione Europea enuncia che "il Titolare del Trattamento è competente per il rispetto dei principi, e in grado di comprovarlo".

4.2. Liceità, correttezza e trasparenza

I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

4.3. Limitazione delle finalità

I dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modalità che non risultino incompatibili o incongruenti con tali finalità determinate.

4.4. Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. Il Titolare del Trattamento deve ad applicare l'anonimizzazione o la pseudonimizzazione ai dati personali, ove possibile, per ridurre i rischi connessi al trattamento e alla conservazione del dato, assicurando maggiori garanzie all'interessato.

4.5. Esattezza

I dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti, nel rispetto delle finalità per le quali essi sono trattati.

4.6. Limitazione del periodo di conservazione

I dati personali devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali essi sono trattati, ovvero fino ad un termine previsto per obbligo di legge, nonché in relazione all'esercizio del diritto di recesso da parte dell'interessato.

4.7. Integrità e riservatezza

Tenendo conto delle tecnologie e di altre misure di sicurezza disponibili, dei costi di attuazione e la probabilità e gravità dei rischi per i dati personali, il Titolare del Trattamento deve mettere in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato per i dati personali, inclusa la protezione dalla distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati.

4.8. Responsabilizzazione

In ordine al principio di *accountability*, il Titolare del Trattamento dei dati personali è competente e vigila circa il rispetto dei principi sopra descritti, e deve essere sempre in grado di comprovarlo.

4.9. Diritti dell'interessato

Secondo le disposizioni del Regolamento Generale per la Protezione dei Dati Personali, ove applicabile, l'interessato ha i seguenti diritti nei confronti del Titolare del Trattamento:

- ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di ottenere l'accesso ai dati personali (Diritto di accesso, articolo 15);
- ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo (Diritto di rettifica, articolo 16);
- ottenere la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del Trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussistono determinate condizioni (Diritto alla cancellazione o all'oblio, articolo 17);
- ottenere la limitazione del trattamento in determinate ipotesi (Diritto alla limitazione del trattamento, articolo 18);
- ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti e ha il diritto di trasmettere tali dati a un altro Titolare del Trattamento, senza impedimenti da parte del Titolare del Trattamento cui li ha forniti, in determinati casi (Diritto alla portabilità dei dati personali, articolo 20);
- opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano (Diritto di opposizione, articolo 21);
- ricevere senza ingiustificato ritardo comunicazione della violazione dei dati personali subita dal Titolare del Trattamento (articolo 34);
- revocare il consenso in qualsiasi momento (Condizioni consenso, articolo 7), qualora la base giuridica del trattamento sia definita da esplicito espressione consenso da parte dell'interessato (ex articolo 6, paragrafo 1, lettera a;
- proporre reclamo all'Autorità di Controllo (articolo 77);
- adire alle opportune sedi giudiziarie (articoli 77 e 78).

4.10. Modalità di esercizio dei diritti

Quando l'interessato richiede al Titolare del Trattamento di esercitare un proprio diritto o più specificatamente di correggere, modificare o distruggere le registrazioni dei dati personali, il Titolare del Trattamento deve garantire che tali richieste siano gestite entro un

ragionevole lasso di tempo, apprezzabile in 30 giorni dalla ricezione della richiesta. L'organizzazione, nell'esercizio della propria titolarità del trattamento, può annotare tali richieste e tenerne un registro.

5. Informativa sul trattamento dei dati personali

5.1 Informativa per utenti e visitatori del portale web

Nel rispetto degli articoli 12, 13 e 14 del Regolamento Europeo 679 del 2016, il Titolare del Trattamento di un portale web che si trovi a trattare dati personali deve avere una propria informativa sul trattamento dei dati personali dedicata ai visitatori ed agli utenti del portale web. Tale informativa potrà essere pubblicata in una pagina dedicata o all'interno di una sezione del portale dedicata alla protezione dei dati personali, raccogliente informative, moduli, funzioni e politiche adoperate dal Titolare del Trattamento in ordine al rispetto dei dispositivi comunitari e nazionali in materia di protezione dei dati personali.

I dati personali possono essere trattati solo in seguito ad esplicita autorizzazione dell'interessato al trattamento dei dati personali (consenso) ovvero allorquando sussistano legittime basi giuridiche per il trattamento dei dati personali, in conformità con quanto disposto dagli articoli 6 e 9 del Regolamento Europeo 679 del 2016.

Al momento della raccolta dei dati personali per qualsiasi tipo di attività di trattamento il Titolare del Trattamento è responsabile dell'informare adeguatamente gli interessati di quanto segue:

- i tipi di dati personali raccolti;
- le finalità del trattamento;
- i metodi di trattamento;
- i diritti degli interessati riguardo ai loro dati personali;
- il periodo di trattamento e conservazione;
- i potenziali trasferimenti (anche di natura internazionale) dei dati;
- se i dati saranno condivisi con terzi;
- le misure di sicurezza adottate per proteggere i dati personali.

Laddove i dati personali siano trasferiti in un paese terzo in base alla politica di trasferimento transfrontaliero dei dati, l'Informativa sul trattamento dei dati personali dovrà esplicitamente menzionare tale attività di trasferimento ed indicare chiaramente dove e a quali soggetti i dati personali vengono trasferiti.

Nel caso in cui vengano raccolti dati personali appartenenti a categorie particolari (sensibili), il Titolare del Trattamento deve assicurarsi che l'Informativa sul trattamento dei dati personali riporti esplicitamente lo scopo per il quale tali dati personali sensibili vengono raccolti e la relativa base giuridica che legittimi il trattamento.

I dati personali devono essere trattati solo per le finalità per cui sono stati originariamente raccolti dal Titolare del Trattamento.

Nel caso in cui il Titolare del Trattamento decida trattare i dati personali raccolti per un altro scopo, esso dovrà informare in forma chiara e concisa l'interessato dell'uso per tale ulteriore

finalità e richiedere, ove necessario, ulteriore manifestazione di consenso. Qualsiasi richiesta di questo tipo deve includere lo scopo originale per cui sono stati raccolti i dati personali e le nuove o aggiuntive finalità. La richiesta deve includere anche il motivo del cambiamento di scopo/i.

Al fine della più corretta informazione all'interessato, l'informativa riporterà sempre l'ultima data di aggiornamento ed il progressivo di revisione, rimandando, eventualmente, con dei collegamenti ipertestuali le precedenti revisioni pubblicate.

5.1.1. Concisa, trasparente, intelligibile e facilmente accessibile

L'obbligo di fornire agli interessati le informazioni e le comunicazioni in forma "concisa e trasparente" implica che il Titolare del Trattamento presenti le informazioni in maniera efficace e succinta al fine di evitare un subissamento informativo. Tali informazioni dovrebbero essere differenziate nettamente da altre che non riguardano la vita privata, quali clausole contrattuali o condizioni generali d'uso. Nell'ambiente online l'utilizzo di una informativa sul trattamento dei dati personali stratificata consentirà all'interessato di consultarne immediatamente la specifica sezione desiderata, senza dover scorrere ampie porzioni di testo alla ricerca di un argomento in particolare.

L'obbligo di fornire informazioni "intelligibili" implica che risultino comprensibili a un esponente medio del pubblico cui sono dirette. L'intelligibilità è strettamente connessa all'obbligo di utilizzare un linguaggio semplice e chiaro. Il titolare dei dati responsabilizzato saprà su che tipo di persone raccoglie informazioni e potrà utilizzare tali conoscenze per stabilire che cosa è probabile che il pubblico in questione comprenda.

Una considerazione centrale al principio della trasparenza è che l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano. Ciò costituisce un aspetto importante del principio di correttezza di cui all'articolo 5, paragrafo 1, del regolamento ed è altresì connesso al considerando 39, il quale stabilisce che «opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali».

In particolare per il trattamento di dati in casi complessi, tecnici o inattesi, la posizione del Gruppo è che, oltre a fornire le informazioni prescritte agli articoli 13 e 14, il Titolare del Trattamento debba dichiarare in una sede distinta, in un linguaggio privo di ambiguità, quali saranno le principali conseguenze del trattamento, in altre parole, quale tipo di effetto sull'interessato, descritto in una informativa sulla privacy, avrà concretamente il trattamento specifico. Conformemente al principio di responsabilizzazione e in linea con il considerando 39, il Titolare del Trattamento dovrebbe valutare se questo tipo di trattamento presenti per le persone fisiche rischi particolari da segnalare loro. Ciò può contribuire a offrire una panoramica dei tipi di trattamento che potrebbero avere l'impatto più forte sui diritti e libertà fondamentali degli interessati in relazione alla protezione dei dati personali che li riguardano.

L'elemento della "facile accessibilità" implica che l'interessato non sia costretto a cercare le informazioni, ma che anzi gli sia immediatamente chiaro dove e come queste siano accessibili, ad esempio perché gli sono fornite direttamente, un *link* lo dirige verso di esse o le informazioni sono contrassegnate chiaramente oppure perché le informazioni si configurano come risposta a una domanda in linguaggio naturale (ad esempio in una informativa sulla privacy stratificata online: in FAQ, provvista dell'utilizzo di icone od info grafiche indicative, ovvero mediante *pop-up* contestuali che si attivano quando l'interessato compila un modulo online oppure, in un contesto digitale interattivo, attraverso un'interfaccia *chatbot*, etc.).

5.1.2. Rendere un'informativa in ambiente digitale

L'utilizzo di informative sulla privacy digitali stratificate non è l'unico mezzo elettronico scritto cui il Titolari del Trattamento può ricorrere. Possono essere utilizzati codici QR stampati su prodotti o documenti, mentre altri mezzi elettronici includono pop-up contestuali "*just-in-time*", notifiche *touch 3D* o *hover-over* e apposite *dashboard*. Gli strumenti elettronici non scritti che possono essere utilizzati in aggiunta alla informativa sulla privacy stratificata potrebbero includere video e notifiche vocali. Gli "altri mezzi" non necessariamente elettronici potrebbero comprendere, ad esempio, vignette, info grafica o diagrammi. Se le informazioni finalizzate alla trasparenza sono dirette specificamente ai minori, il Titolare del Trattamento dovrebbe valutare quali tipi di misure possano essere accessibili in modo particolare ai minori (tra gli altri, ad es., fumetti, vignette, pittogrammi, animazioni, ecc.).

Il Titolare del Trattamento deve prendere una decisione sulla modalità e sulla forma appropriata per fornire le informazioni tenendo conto di tutte le circostanze della raccolta e del trattamento dei dati. In particolare, le misure appropriate dovranno essere valutate alla luce dell'esperienza dell'utente con il prodotto/servizio, vale a dire tenendo conto del dispositivo utilizzato, della natura delle interfacce utente/interazioni con il Titolare del Trattamento (il cosiddetto "percorso utente") e delle limitazioni che tali fattori implicano.

5.1.3. Notifiche push e notifiche pull

Un altro possibile modo per fornire informazioni finalizzate alla trasparenza è attraverso l'uso di notifiche *push* e *pull*. Le notifiche *push* implicano la fornitura di messaggi *just in time*, mentre quelle *pull* facilitano l'accesso alle informazioni con metodi quali la gestione dei permessi, *dashboard* per la privacy e tutorial per saperne di più. L'interessato può così fruire di un'esperienza maggiormente incentrata sull'utente.

Una *dashboard* per la privacy è un punto unico dal quale l'interessato può visualizzare le "informazioni sulla privacy" e gestire le proprie preferenze permettendo o impedendo al servizio in questione determinati usi dei dati che lo riguardano. È particolarmente utile quando l'interessato usa lo stesso servizio su diversi dispositivi, perché dà accesso ai dati personali e la possibilità di controllarli a prescindere dall'uso fatto del servizio. Il fatto che l'interessato possa modificare manualmente le impostazioni sulla privacy tramite un'apposita *dashboard* può inoltre facilitare la personalizzazione della informativa sulla privacy, che sarà in grado di rispecchiare solo i tipi di trattamento che si verificano per quel particolare interessato.

È preferibile incorporare una *dashboard* per la privacy nell'architettura preesistente di un servizio perché questo favorirà l'intuitività dell'accesso e dell'uso e potrà contribuire a incoraggiare gli utenti a servirsi di queste informazioni, esattamente come farebbero con altre componenti del servizio. Può essere un modo efficace di dimostrare che le "informazioni sulla privacy" costituiscono un elemento necessario e parte integrante di un servizio anziché un lungo elenco di termini legalistici.

La notifica *just-in-time* è utilizzata per fornire "informazioni sulla privacy" specifiche in maniera *ad hoc*, vale a dire come e quando è più importante per l'interessato leggerle. Questo metodo è utile per fornire informazioni in vari momenti del processo di raccolta dei dati, favorisce una fornitura delle informazioni a blocchi assorbibili facilmente e riduce l'affidamento su un'unica informativa sul trattamento dei dati personali piena d'informazioni difficilmente comprensibili fuori contesto. Ad esempio, se l'interessato acquista un prodotto online, possono essere fornite brevi informazioni esplicative in *pop-up* che accompagnano le pertinenti sezioni del testo. Accanto al campo che chiede il numero di telefono dell'interessato, le informazioni potrebbero ad esempio spiegare che il dato è raccolto soltanto per disporre di un contatto con riferimento all'acquisto e che sarà comunicato solo agli addetti del servizio di consegna.

5.2 Consenso dell'interessato come base giuridica

Ogni volta che il trattamento dei dati personali si basa sul consenso dell'interessato, o su altri motivi legittimi, il Titolare del Trattamento è responsabile della conservazione di una registrazione di tale consenso. Il Titolare del Trattamento è altresì responsabile della fornitura, agli interessati, di modalità per esplicitare il proprio consenso, così da informarli e garantendo che il loro consenso (ogni volta che il consenso venga utilizzato come base legale per il trattamento) possa essere revocato in qualsiasi momento. Il Titolare del Trattamento nell'esercizio del trattamento deve garantire che i metodi di raccolta del consenso siano conformi alle vigenti normative nazionali e comunitarie in materia.

Il consenso dell'interessato può essere raccolto univocamente soltanto per una singola finalità, sono da ritenersi invalide le espressioni di consenso per diverse finalità aggregate.

Laddove la raccolta di dati personali – connessa ad un trattamento la cui base giuridica è il consenso dell'interessato – si riferisca a un minore di età inferiore ai 16 anni, il Titolare del Trattamento deve garantire che il consenso del titolare della responsabilità genitoriale sia fornito prima della raccolta.

Si ricorda che i trattamenti vincolati alla acquisizione di un consenso espresso da parte dell'interesso devono interrompersi alla data ultima di trattamento prevista in informativa, fatto salvo rinnovo del consenso da parte dell'interessato (ad esempio, non esaustivo, per le attività di trattamento in ambito di marketing ed informazione commerciale vige il limite massimo di utilizzo dei dati personali in 24 mesi dall'acquisizione del consenso).

6. Acquisizione dei dati personali sul portale web

6.1. Gestione dei moduli di acquisizione dei dati personali

Se sul portale web del Titolare del Trattamento dei dati personali sono presenti dei moduli di acquisizione dei dati personali (*compila form*, *contact form*, questionari o creazione di profilo utente), dovrà verificarsi in base allo specifico caso l'opportuna presenza di *checkbox* finalizzati:

a) alla presa visione dell'informativa sul trattamento dei dati personali e la relativa indicazione delle finalità del trattamento;
b) all'accettazione al trattamento dei dati personali per attività di trattamento la cui base giuridica sia rappresentata del consenso dell'interessato;
c) alla verifica dell'età dell'interessato.

In tal misura l'obbligatorietà del primo *checkbox* è da rintracciarsi nell'articolo 13, paragrafo 1 del Regolamento Europeo 679 del 2016 statuente che «in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del Trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti» tutte le informazioni necessarie ad identificare i principi e le modalità di trattamento.

Il secondo *checkbox* è da proporsi solo quando il Titolare del Trattamento sia a processare i dati per finalità la cui base giuridica sia da verificarsi nel libero consenso da parte dell'interessato (ad esempio per attività di marketing oppure per attività relative alla newsletter). Difatti, allorquando, il Titolare del Trattamento sia a definire che sui dati di contatto dell'interessato è volontà del medesimo proporre a quest'ultimo anche la possibilità di utilizzarli per attività di informazione commerciale, vi si pone l'inviolabile necessità di apporre uno specifico *checkbox*, facoltativo per l'interessato e non preticcato. Si tenga inoltre presente che in tal circostanza si dovranno adottare tutte le misure tecnico-logiche affinché il Titolare sia sempre «in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali» (articolo 7, paragrafo 1, Reg. UE 2016/679) ed affinché si conceda all'interessato il «diritto di revocare il proprio consenso» (articolo 7, paragrafo 3, Reg. UE 2016/679).

Per il terzo *checkbox*, invece, allorquando non si verifichi una identificazione "a monte" dell'età dell'interessato sul portale web (ad esempio utilizzando una registrazione dell'età in caso di creazione di un profilo-utente) – facendo scorta sul considerando 38 del Regolamento Europeo 679 del 2016, il quale prevede per i minori «una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi [...] in relazione al trattamento dei dati personali – tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing [...] e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi» – il *checkbox* per la verifica dell'età dell'interessato è da ritenersi obbligatorio allorquando sia presente il *checkbox* per il trattamento di dati personali in relazione a finalità di marketing. Se il richiedente ha meno di 16 anni non può procedere con la comunicazione dei propri dati, a meno che il form non sia integrato anche da ulteriori campi di autorizzazione da parte dei genitori o tutore legale.

In ogni caso è comunque necessario mantenere traccia e data certa circa il corretto rilascio da parte dell'utente del dato salvando le informazioni di rilascio (log) all'interno di un database, come meglio specificato in seguito.

Per una migliore comprensione, si rimettono in seguito degli esempi esplicativi, non esaustivi, per il corretto posizionamento dei *checkbox*.

Sotto i form destinati alla lead generation per attività di marketing (o newsletter):
☐ Ho preso visione dell'informativa per il trattamento dei dati personali *(da collegare al link della policy privacy)* ed acconsento al trattamento dei miei dati personali per le finalità di marketing (o per l'iscrizione alla newsletter)
☐ Ho più di 16 anni.

Sotto i form destinati alla creazione dei profili utente o all'acquisto prodotti/servizi:
☐ Ho preso visione dell'informativa per il trattamento dei dati personali *(da collegare al link della policy privacy)* e dei termini e condizioni d'uso del portale (ove presente inserire in link dei termini e delle condizioni d'uso del portale) e sono consapevole che i miei dati verranno trattati per _____ (inserire la/le finalità per cui si effettua il trattamento e la cui base giuridica non sia da verificarsi nel consenso dell'interessato);
☐ Acconsento al trattamento dei miei dati personali anche per le finalità di marketing e per l'iscrizione alla newsletter (se si effettuano attività di marketing);
☐ Acconsento al trattamento dei miei dati personali anche per le finalità di ricerche di mercato e rilievo del gradimento (se si effettuato attività di ricerche di mercato e rilievo del gradimento);
☐ Ho più di 16 anni (allorquando non sia presente un sistema già integrato di verifica dell'età dell'utente).

Sotto i form destinati all'invio di messaggi (mailbox) o richieste:
☐ Ho preso visione dell'informativa per il trattamento dei dati personali *(da collegare al link della policy privacy) e* sono consapevole che i miei dati personali ivi rilasciati verranno trattati per l'invio e il riscontro alla mia richiesta o messaggio.

Sotto i form destinati all'invio di curriculum e candidature lavorative:
☐ Ho preso visione dell'informativa per il trattamento dei dati personali dei candidati *(da collegare al link della policy privacy dei candidati) e* sono consapevole che i miei dati personali ivi rilasciati verranno trattati per la ricezione del mio curriculum e della mia candidatura lavorativa.

6.2. Rimodulazione messaggi opt-out

Eventuali messaggi sponsorizzati e moduli funzionanti in modalità opt-out (e cioè i moduli che appaiono quando il cursore del mouse si muove verso la parte superiore della pagina per chiuderla) dovranno essere riadattati ad opt-in opzionale.

7. Dati della navigazione

7.1. Registrazione dei log

Dal momento che la presa visione ed ancor di più il consenso deve essere prestato in modo espresso ed inequivocabile dall'utente, i moduli inseriti nel sito web non potranno più contenere un consenso di default (le caselle dei *checkbox* non potranno essere preticcate).

Al fine di poter verificare se un utente ha acconsentito ad un trattamento dei dati personali tali espressioni di consenso dovranno essere conservate all'interno di un database, ove sia possibile aggregare dati, allorquando disgregati, al fine di verificare il rilascio del consenso.

Ad Esempio: Mario Rossi ha acconsentito al trattamento dei propri dati per la newsletter ticcando l'apposito *checkbox* di consenso. Il database mi conserva il log - nome: Mario, il log – cognome: Rossi, e l'azione: il rilascio del consenso (eventualmente con indicazione dell'ora e dell'indirizzo IP), successivamente riaggregando le informazioni posso verificare da database che Mario Rossi mi ha rilasciato il proprio consenso al trattamento dei propri dati per l'iscrizione alla newsletter.

Il portale web dovrà essere dotato di un proprio database che faciliti la richiesta di cancellazione dei dati personali, ovvero di limitazione od opposizione al trattamento

Ad esempio: in eventuali aree riservate al profilo-utente, l'interessato avrà a disposizione uno o più pannelli per la gestione delle proprie preferenze in ordine al trattamento dei suoi dati personali (garantendo così l'esercizio dei diritti di opposizione e/o di limitazione) ovvero una funzione per l'eliminazione del proprio profilo-utente (in ordine al diritto di cancellazione o di oblio).

È necessaria, inoltre, l'implementazione di un sistema di verifica dei dati degli utenti/visitatori che consenta, da parte del Titolare del Trattamento, una notifica immediata nel caso in cui vengano violati i dati personali degli interessati.

7.2. Gestione ed attivazione dei cookie

Secondo il Regolamento Europeo 679 del 2016 i dati personali sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica: nome e cognome, foto, indirizzi email, dettagli bancari, interventi su siti web, su social network, informazioni mediche o indirizzi IP.

Per questo anche i cookie devono essere considerati dei dispositivi per il trattamento dei dati personali e devono essere gestiti come segue:

- i dati personali non possono essere tracciati o profilati prima che l'utente abbia dato il consenso esplicito;
- devono essere specificati tutti i tracciamenti dei dati personali attivi sulle pagine del sito web;
- ogni autorizzazione deve essere salvata e registrata per provare che è stata concessa;
- la revoca del consenso deve essere facile da effettuare, anche in un secondo momento;
- gli utenti del sito web devono essere informati in un linguaggio semplice su:

a) chi riceve i dati e su come sono usati;
b) la data di scadenza dei cookie.

Inoltre la *cookie policy* deve contenere la lista di tutti i cookie (o qualsiasi altro script utilizzato per identificare e/o profilare l'utente) presenti sulle pagine del sito e per ognuno di essi: chi riceve i dati, per cosa sono utilizzati e la data di scadenza.

Tecnicamente i *browser* non riescono a leggere lo scopo di un cookie (come esso viene utilizzato) e non possono fornire una sua descrizione in un "linguaggio semplice" così come è richiesto nel Regolamento Generale per la Protezione dei Dati Personali.

I *browser* non possono registrare tutti i cookie presenti in un intero sito all'accesso, ma solo alla navigazione della pagina in cui essi insistono; non possono gestire automaticamente i consensi in base alle preferenze rilasciate su altri portali web e non possono, inoltre, fornire il salvataggio dei consensi: pertanto i gestori dei siti web dovranno provvedere a tali funzioni in funzione di quanto disposto dalla regolamentazione comunitaria e dai provvedimenti in materia da parte dell'Autorità Garante per la Protezione dei Dati Personali.

Per maggiori informazioni sulla corretta gestione dei cookie si rimanda alla **Linea Guida sull'"Utilizzo dei cookie sul portale web aziendale e di altri sistemi di tracciamento"**.

8. Compila form connessi a provider esterni per servizi di newsletter

Se i compila form sono collegati a provider esterni – ad esempio l'acquisizione del dato giunge direttamente ad un fornitore di parte terza che fornisce il servizio di newsletter – il rilascio del consenso potrà essere verificato anche sulla piattaforma esterna, attraverso i profili di contatto iscritti nelle liste. Nel caso in cui il form di iscrizione alla newsletter sia direttamente collegato ad un provider esterno è consigliato inserire in seguito al medesimo i riferimenti del fornitore del servizio di newsletter, linkando anche la sua informativa privacy.

Il Titolare del Trattamento all'interno della newsletter dovrà provvedere all'apposizione di un *disclaimer* per le comunicazioni riferito al trattamento ed alla protezione dei dati personali ed un metodo di disiscrizione rapida, atto a garantire il diritto di opposizione riconosciuto all'interessato.

8.1. Iscrizione alla newsletter per clienti

In relazione all'invio di newsletter ai propri clienti, anche senza rilascio di esplicito consenso, si ricorda che l'articolo 130 del D.Lgs 196 del 2003, come modificato dal D.Lgs 101 del 2018, al paragrafo 4, statuisce che se «il Titolare del Trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni», addizionando che «l'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente paragrafo, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente».

In tal misura la base giuridica che sarebbe a legittimare il trattamento del dato di corrispondenza elettronica per l'invio di newsletter è da rinvenirsi non più nel consenso dell'interessato ma nel legittimo interesse del Titolare del Trattamento (ai sensi dell'articolo 6, paragrafo 1, lettera f del Regolamento Europeo 679 del 2016) «nel cercare di vendere un maggior numero di prodotti ai suoi clienti» (si veda la sezione III, articolo 3, paragrafo 3 del "Parere 6/2014 sul concetto di interesse legittimo ai sensi dell'articolo 7 della direttiva 95/46/CE" [844/14/IT - WP 217] adottato dal Gruppo di Lavoro articolo 29.

L'applicazione di tale orientamento comporta l'evidenza di tale trattamento all'interno dell'informativa per il trattamento dei dati personali fornita ai clienti frontalmente e l'adozione delle opportune logiche tecniche affinché si consenta l'opposizione al trattamento da parte dell'interessato (come il tasto di disiscrizione rapida presente nel *footer* comunicazione dei principali provider di newsletter e/o un metodo di disiscrizione rapida da porre all'informativa sul trattamento dei dati personali pubblicata sul sito web e/o un pannello di gestione delle preferenze all'interno del profilo utente).

I dati personali e di contatto utilizzati per l'invio della newsletter in ordine al legittimo interesse da parte del Titolare del Trattamento per il mantenimento della propria clientela saranno utilizzati fino ad un massimo di 5 anni dall'anno cui fa riferimento l'ultimo acquisto. L'interessato può comunque opporsi in ogni momento al trattamento.

9. Procedure e sistemi di sicurezza consigliati per il sito web

L'articolo 32 del Regolamento Europeo 679 del 2016 prevede che «tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento e il Responsabile del Trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento».

In questa sezione saranno indicate alcune procedure e sistemi di sicurezza consigliati per il sito web, nel rispetto del principio di *accountability* disposto dal Regolamento Generale per la Protezione dei Dati Personali.

9.1. Fornitore dei servizi di hosting

La scelta di un server hosting certificato in sicurezza è fondamentale per garantire prestazioni e protezione al sito internet. Generalmente il fornitore del servizio server hosting dovrebbe garantire, almeno, l'uso di un *Web Application Firewall*, di Sistemi *IA anti-bot*, di ridondanza e di *Intrusion Detection*, di misure per la protezione da attacchi *DDoS*, di protocolli

crittografati di comunicazione e di tecnologie per garantire la resilienza dei dati e delle informazioni (*Disaster recovery* geografico).

Il Titolare del Trattamento può verificare l'adesione da parte del fornitore a Codici di Condotta o l'acquisizione di meccanismi di Certificazione: come lo standard ISO/IEC 27001 che contiene i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni o lo standard ISO/IEC 27018 – espansione della Norma ISO 27001 – che, nello specifico, riguarda la gestione dei dati personali in relazione alle soluzioni cloud in modalità IaaS, PaaS e SaaS.

Il fornitore del server hosting, a norma dell'articolo 28 del Regolamento Europeo 679 del 2016, si configura come Responsabile del Trattamento dei dati personali: se non autonominato in contratto di fornitura del servizio di hosting, questo dovrà essere nominato Responsabile dal Titolare del Trattamento, in accordo anche con quanto previsto dalla Linea Guida n. 7/20 adottata il 7 luglio 2021 dall'European Data Protection Board sui "concetti di Titolare e Responsabile del Trattamento nel Regolamento Generale per la Protezione dei Dati Personali".

9.2. Soggetto incaricato alla gestione del portale web

Il soggetto incaricato alla gestione del portale web, se esterno alla struttura del Titolare del Trattamento ed allorquando interagente con il trattamento dei dati personali, dovrà – nel rispetto dell'articolo 28 del Regolamento Europeo 679 del 2016 – operare in qualità di Responsabile del Trattamento dei Dati Personali. In tal misura esso dovrà fornire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del regolamento generale sulla protezione dei dati personali, garantendo, altresì, la tutela dei diritti dell'interessato.

I trattamenti da parte di un Responsabile del Trattamento sono disciplinati da un contratto o da altro atto giuridico, che vincoli il Responsabile del Trattamento al Titolare del Trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del Trattamento.

Allorquando il soggetto operante in merito sia interno si applicheranno, invece, i termini disposti dall'articolo 29 Regolamento UE n. 2016/679 e dell'articolo 2-quaterdecies del D.Lgs 196 del 2003, come modificato dal D.Lgs 101 del 2018, individuando il medesimo quale incaricato autorizzato al trattamento dei dati personali, ed operando sicché sotto l'autorità diretta del Titolare del Trattamento.

In caso di sistemi informativi e banche dati operanti in ordine al portale web particolarmente complesse si ricorda che, ai sensi e per gli effetti Provvedimento del 27 novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali, tali operatori potrebbero assumere il ruolo di Amministratore di Sistema.

9.3. Protocollo di comunicazione protetto

Tra le disposizioni da osservare in relazione all'adeguamento del portale web alla normativa comunitaria sulla protezione dei dati personali vi è anche da annoverare l'installazione del

certificato *SSL*: il certificato permette di rendere crittografato, quindi sicuro, il traffico da e verso il sito internet.

L'adozione del protocollo *HTTPS* per l'accesso al portale aziendale garantisce un canale di comunicazione criptato e certificato dal *Transport Layer Security (TLS)* tra il *client* e il *server* e risponde, quindi, all'esigenza di un livello di adeguatezza delle misure di sicurezza richiesta dall'articolo 32, lettera b, del il Regolamento Europeo sulla protezione dei dati: «...capacità di assicurare su base permanente la riservatezza, l'integrità e la disponibilità dei sistemi e dei servizi di trattamento».

Usando questa particolare misura tecnica, il Titolare del Trattamento che utilizza piattaforme web per la comunicazione ed il trattamento dei dati personali adotta il principio di *accountability* introdotto proprio con il Regolamento Europeo 679 del 2016 (si tenga presente che comunque questo non riporta alcuna indicazione esplicita sull'uso del protocollo HTTPS).

9.4. Sistemi antivirus, antimalware e Firewall

I dispositivi e il server hosting utilizzati per l'implementazione, la gestione ed il funzionamento del sito internet aziendale sono target di potenziali attacchi cibernetici. Il Titolare del Trattamento ed i Responsabili del Trattamento incaricati in ordine alla gestione del portale web o alla fornitura del server devono quindi dotarsi delle misure di sicurezza necessarie alla mitigazione di tale rischio: in tal misura adopereranno l'uso di sistemi aggiornati per la prevenzione a virus, malware e ransomware che effettueranno scansioni periodiche e programmate per la rilevazione ed il contrasto ai medesimi.

Se del caso, gli operatori provvederanno all'installazione di firewall di adeguata generazione al fine di contrastare le vulnerabilità dei sistemi informativi connessi alla gestione od al funzionamento del portale web.

9.5. Backup dei dati e delle informazioni

In ordine alla resilienza dei dati personali ed alle misure di contrasto a possibili fattispecie di *data breach* o *disaster recovery*, si dovrà sempre garantire il progressivo, periodico ed automatico salvataggio e *backup* dei file presenti sul server hosting ospitante il portale web e delle informazioni sul database ad esso connesso.

In tal misura il Titolare del Trattamento, con il supporto dei Responsabili del Trattamento incaricati in merito, potrà dotare il portale web di un piano di ripristino dell'operatività e di continuità: definendo le azioni che dovranno essere messe in atto dopo eventi interruttivi o fraudolenti al fine di ripristinare prima possibile la normale operatività del sito internet.

9.6. Content Management System, template e plugin

Se il portale web sviluppato è con un *Content Management System* bisogna verificare che esso sia installato nella versione ufficiale aggiornata alla ultima versione e che piattaforma non interferisca con il corretto od esponga a vulnerabilità il trattamento dei dati personali.

Ugualmente, i *template* o *plugin* sono spesso punti di criticità per la sicurezza del portale web, a tal proposito è consigliato l'uso di temi ed applicativi con licenza d'uso valida, costantemente aggiornati ed implementati e che adottino sufficienti garanzie di sicurezza.

Andrà, anche in questo caso, verificata la possibilità che i gestori dei medesimi possano accedere o meno alle informazioni ed ai dati derivanti dai trattamenti attivi sul portale web.

9.7. Gestione delle chiavi di accesso

Sia per le operazioni di *back-end* da parte dei gestori del portale web, sia per le operazioni di *front-end* da parte di profili-utente dotati di pannelli con accesso a mezzo di *login*, il sistema di funzionamento del sito va dotato di funzionalità specifiche atte a garantire sufficienti misure di sicurezza in ordine alla creazione ed alla conservazione delle chiavi di accesso. In particolar modo il sistema dovrebbe obbligare la creazione di password complesse, come da seguenti parametri:

- utilizzare almeno dodici caratteri;
- utilizzare almeno un carattere numerico;
- utilizzare almeno un carattere alfabetico maiuscolo e almeno uno minuscolo;
- utilizzare almeno un carattere speciale;
- le ultime tre password non devono essere riutilizzate;

ovvero provvedere alla periodica modifica della chiave di accesso. In ogni caso la base dati nella quale verranno iscritte le informazioni di *login* devono sempre prevedere al loro interno protezione ed anonimizzazione con funzione *hash* crittografica.

Per una sicurezza incrementale può essere sempre previsto l'introduzione di un metodo di accesso che si basi sull'utilizzo congiunto di due metodi di autenticazione individuali (autenticazione a due fattori).

9.8. Crittografia del server e del database

La verifica della crittografia e delle misure di protezione – si consulti il successivo paragrafo – di cui sono dotati server hosting e database utilizzati per il funzionamento del portale web è precondizione necessaria per la sicurezza del medesimo. Si consiglia, in merito, di conservare i certificati di garanzia relativi alle misure di sicurezza consegnati o pubblicati dai fornitori ed i termini e le condizioni contrattuali stipulate con i provider.

9.9. Anonimizzazione e Pseudoanonimizzazione

Lo scopo dell'anonimizzazione dei dati personali è rendere impossibile l'identificazione attraverso una serie di dati anonimi, anche allorquando si agisca con l'ausilio dei dati originali. In tal misura, i dati resi anonimi non sono considerati dati personali.

I seguenti metodi sono tipicamente adoperati – o simultaneamente od alternativamente, anche in funzione del grado di rischio e dell'uso previsto dei dati – in ordine alle misure di anonimizzazione:

- Sostituzione delle *directory*: modifica del nome delle persone integrate nei dati, mantenendo la coerenza tra i valori, come "codice postale + città", "età + sesso".
- *Scrambling*: comporta una miscelazione o l'offuscamento delle lettere. A volte il processo può essere reversibile. (Ad esempio: Roberto potrebbe diventare Betroro).
- Mascheramento: consente di nascondere una parte dei dati con caratteri casuali o altri dati.

- Sfocatura: un'approssimazione dei valori dei dati per rendere il loro significato obsoleto e/o rendere impossibile l'identificazione degli individui.
- Privacy differenziale: questo metodo può essere utilizzato ogni volta che il soggetto che effettua il trattamento fornisce a terzi l'accesso a una serie di dati anonimi. Una copia dei dati originali rimane presso il soggetto che effettua il trattamento e il destinatario terzo riceve solo una serie di dati anonimi.
- Aggregazione: un interessato è raggruppato con diversi altri interessati che condividono alcuni o tutti i dati personali.

La pseudonimizzazione intende migliorare la privacy sostituendo i campi di identificazione all'interno di una registrazione di dati con uno o più identificatori artificiali o pseudonimi. Pertanto, la pseudonimizzazione riduce, ma non elimina completamente, la possibilità di collegare una serie di dati con l'identità di un interessato. Metodi di pseudonimizzazione appropriati sono:

- Cifratura (con l'uso di un codice segreto): i dati vengono cifrati con l'uso di un codice segreto. Il possessore del codice segreto può facilmente re-identificare gli interessati decodificando la serie di dati.
- Funzioni crittografiche di *hash*: utilizzate per mappare dati di qualsiasi dimensione su codici di dimensioni fisse (si noti che esistono più tecniche di *hashing* (ad esempio *hash* "salati", HMAC, ecc.).
- *Tokenizzazione*: il processo di sostituzione di un elemento di dati sensibili con un equivalente non sensibile, denominato *token*. Il token è un riferimento (ovvero un identificatore) che esegue la mappatura dei dati sensibili tramite un sistema di tokenizzazione. Il sistema di tokenizzazione fornisce alle applicazioni di elaborazione dati l'autorizzazione e le interfacce per richiedere token o per riattivare i dati sensibili.

9.10. Localizzazione del server hosting, del database e dei provider

Ulteriore condizione necessaria atta a garantire la protezione dei dati personali degli interessati è la verifica della posizione fisica dei server hosting e dei database utilizzati per la gestione ed il funzionamento del sito web e dei fornitori di servizi di parte terza interagenti con il trattamento dei dati personali operante sul portale.

In particolar modo è necessario validare se essi siano localizzati o meno all'interno dell'Unione Europeo o dello Spazio Economico Europeo, difatti, il Regolamento Generale per la Protezione dei Dati Personali prevede che il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale deve essere effettuato nel rispetto di specifiche condizioni affinché non sia pregiudicato il livello di protezione delle persone fisiche garantito dal Regolamento Europeo 679 del 2016.

In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali possono essere effettuati solo quando sono rispettate tutte le condizioni e le disposizioni di cui gli articoli da 45 a 49 del Regolamento Generale per la Protezione dei Dati Personali.

10. Validità e gestione del documento

Questo documento ha effetto dal 20/05/2024.

Il responsabile per questo documento è la ACEN - Associazione Costruttori Edili Napoli, Titolare del Trattamento, la quale deve controllare e, se necessario, aggiornare il presente documento con frequenza annuale.

Responsabile della Protezione dei Dati	Legale Rappresentante
ACEN - Associazione Costruttori Edili Napoli	ACEN - Associazione Costruttori Edili Napoli
Dott. Guglielmo Pulcini	Ing. Angelo Lancellotti
_____	_____

Moduli realizzati sulla base di questo documento

1. Informativa sul trattamento dei dati personali per portale web
2. Informativa sui cookie per portale web