REGOLAMENTO IN MATERIA DI PROTEZIONE E SICUREZZA DEL TRATTAMENTO DATI

Il presente documento è redatto in conformità al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27-04-2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [lo stesso ha abrogato la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)], e recepito in Italia per effetto del D.lgs. 101/2018, emanato a seguito di L.D. 163/2017.

1 PREAMBOLO

A seguito dell'entrata in vigore:

- del Regolamento UE 679/2016, in materia di protezione dei dati personali - pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 ed entrato in vigore il 24 maggio 2016 e che è applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018 – (in seguito anche solo *GDPR*)
- del D.lgs. 101/2018, che recepisce il GDPR ed emanato a seguito della Legge Delega 163/2017,

la **DOC Service S.r.l.** (di seguito anche *DOCS*, *Società*, *Impresa* od *Organizzazione*) ha deciso di munirsi di un nuovo Regolamento in materia di Protezione e Sicurezza del Trattamento Dati, al fine di adeguarsi alla regolamentazione dell'Unione Europea e alla legislazione nazionale vigente (in seguito *normativa applicabile*).

Il GDPR disciplina le modalità di trattamento dei dati personali delle persone fisiche sotto un triplice profilo:

- il consenso informato nel momento acquisitivo dei dati;
- il corretto utilizzo
- la tutela nel momento di circolazione dei dati.

Giusto infatti sottolineare che il GDPR si ispira al riconosciuto e tutelato diritto dell'individuo di disporre dei propri dati, quali aspetti del fondamentale diritto di identità e personalità (art. 16 del TFUE, art. 8 della carta dei Diritti Fondamentali).

2 PRINCIPI INTRODOTTI DAL GDPR

2.1 ACCOUNTABILTY

Il termine *accountability* indica il Principio su cui si fonda il GDPR.

Si tratta della responsabilità che il Titolare del trattamento ha e che si manifesta attraverso il garantire l'efficacia della tutela predisposta mediante azioni che includono il riesame e l'aggiornamento costante di tutte le condizioni adottate.

2.2 PRIVACY BY DESIGN AND BY DEFAULT

L'espressione indica il principio per il quale la riservatezza (in seguito anche *privacy*) deve essere tenuta presente e incorporata a partire dalla progettazione di un processo aziendale in riferimento al quale vanno strutturate appositamente le relative applicazioni informatiche di supporto.

In base a tale principio l'Organizzazione costruisce i suoi sistemi informatici e le sue pratiche basate direttamente sulla *privacy* sin dalla fase di progettazione, garantendo in tal modo l'esistenza della *privacy* sin dall'inizio.

2.3 PSEUDONIMIZZAZIONE

È il principio per il quale viene favorita la tutela dell'individuo e dei suoi dati personali.

Consiste "nel 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 psuedonimizzazione non è da confondersi con la anonimizzazione.

2.4 PROFILAZIONE

È il principio per il quale il Titolare del trattamento svolge una qualsiasi forma di trattamento automatizzato di dati personali e consistente nell'utilizzo di tali dati per valutare aspetti personali (es.: analisi o previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti della persona).

In tali circostanze Titolare del trattamento deve darne espressa informativa all'Interessato, raccogliendo relativo espresso consenso.

2.5 PORTABILITÀ DEI DATI

È il principio per il quale l'Interessato hai il diritto di chiedere (in caso di passaggio da un Titolare del trattamento a un altro) che i dati vengano comunicati dal precedente Titolare del trattamento, al successivo.

Questo principio è una novità assoluta introdotta dal GDPR.

2.6 DIRITTO ALL'OBLIO E CONSERVAZIONE LIMITATA

È il principio per il quale i dati dell'Interessato devono essere conservati per il tempo strettamente necessario alla attuazione delle finalità per le quali nella Informativa è stato dichiarato che detti dati sono stati raccolti.

L'Interessato ha il diritto di ottenere, in qualunque momento, la cancellazione dei propri dati *on line* se i dati sono trattati illecitamente, se sono stati rilasciati sulla base del consenso, se l'interessato si oppone al loro trattamento, se i dati non sono più necessari allo svolgimento delle finalità per le quali sono stati raccolti.

Il diritto all'oblio è escluso qualora si tratti di informazioni di interesse generale o necessarie per finalità storiche, statistiche o scientifiche.

2.7 DATA BREACH – VIOLAZIONE DEI DATI PERSONALI.

È il principio per il quale il Titolare del trattamento ha l'obbligo, in caso di violazione dei dati personali[1], di svolgere una propria valutazione dell'impatto che l'evento negativo può avere sui dati interessati dal verificarsi di detto rischio.

A seguito di tale valutazione, il Titolare del trattamento notifica la medesima (obbligatoriamente solo quando ritenga che da tale violazione derivino rischi per i diritti e le libertà delle persone) entro massimo 72 ore (e comunque quanto prima) al Garante.

In ogni caso, in presenza di violazioni, il Titolare del trattamento ha l'obbligo di documentare le violazioni, anche quando non notificate al Garante.

Le misure di sicurezza da adottarsi preliminarmente in ipotesi di *data breach* devono "garantire un livello di sicurezza adeguato al rischio" del trattamento[2] (non è più possibile fare riferimento generico all'adozione di misure minime di sicurezza – *N.d.R.*). Questa valutazione è rimessa, caso per caso, al Titolare e al Responsabile del trattamento in relazione ai rischi che vengono di volta in volta specificamente rilevati, anche seguendo le linee guida che l'*Authority* in tema di riservatezza emana.

Al fine di dotarsi di una maggiore tutela, in DOCS vi è un codice di condotta cui riferirsi (vedere "Procedure, P-7500" in vigore).

3 DEFINIZIONI

L'art. 4 del GDPR fornisce le seguenti definizioni:

- **Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, dati relativi alla ubicazione, un identificativo online o ad uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **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.
- **Limitazione di Trattamento**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **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;

[1] *Nota bene: La violazione può essere rappresentata da qualunque rischio che provochi "impatti negativi sulle libertà e i diritti degli interessati" (definizione dell'Autority Garante Italiana)*

[2] *Nota bene: Vedere Articolo 32, § 1 del GDPR.*

- **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;
- **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;
- **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;
- **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;
- **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;
- **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;
- **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;
- **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;
- **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;
- **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;
- **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;
- **Stabilimento principale:**
  a) 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;

b) 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;

- **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;
- **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;
- **Gruppo imprenditoriale**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- **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;
- **Autorità di controllo**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
- **Autorità di controllo interessata**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
  a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
  b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
  c) un reclamo è stato proposto a tale autorità di controllo;
- **Trattamento transfrontaliero**:
  a) 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
  b) 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;
- **Obiezione pertinente e motivata**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

- **Servizio della società dell'informazione**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;
- **Organizzazione internazionale**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

4 TRATTAMENTO DEI DATI IN DOCS

La **DOCS** dichiara di essere unico Titolare del trattamento dei dati raccolti e conservati c/o di essa. Asserisce inoltre di trattare i dati in conformità con le indicazioni di legge e quindi in maniera lecita (cioè fondata sul consenso dell'interessato) corretta (attraverso l'informazione all'Interessato circa la raccolta, l'utilizzo e altri eventuali successivi trattamenti dei dati forniti) trasparente (attraverso modalità predefinite e rese note all'interessato in modo chiaro, semplice e accessibile).

La **DOCS** dichiara:

- di raccogliere i dati per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- di raccogliere dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (in osservanza del principio della «minimizzazione dei dati» espresso dal GDPR);
- di raccogliere dati esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (in osservanza del principio di «esattezza» espresso dal GDPR);
- di conservare i dati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici[3], fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato (in osservanza del principio della «limitazione della conservazione» espresso dal GDPR);
- di trattare i dati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, in modo tale da evitare trattamenti non autorizzati o illeciti e difendere i dati dalla perdita, dalla distruzione o dal danno accidentali (in osservanza del principio della «integrità e riservatezza» espresso dal GDPR).

La **DOCS**, sebbene la tutela legale offerta dalla normativa in materia di trattamento dei dati si riferisce ai soli dati delle Persone fisiche, si impegna a prestare attenzione nelle ipotesi in cui attraverso i dati delle persone giuridiche si acquisiscano dati di persone fisiche. In queste ipotesi.

La **DOCS** dichiara di tutelare i dati personali di persone fisiche acquisiti per via mediata dalle persone giuridiche.

- **Tipologia di dati raccolti**

La **DOCS** dichiara, qui di seguito, l'ambito specifico del trattamento dati che adopera in relazione alla attività svolta.

[3] *Nota bene: La conservazione avviene in conformità all'Articolo 89, paragrafo 1, del GDPR.*

L'Organizzazione tratta dati personali con esclusione di quelli genetici, biometrici o relativi alla salute.

L'Organizzazione raccoglie dati con finalità dirette alle attività di realizzazione di servizi di progettazione, installazione e manutenzione di impianti elettronici in genere (es.: antintrusione, controllo degli accessi, videosorveglianza, protezione antincendio).

In particolare, raccoglie i dati necessari al perseguimento delle seguenti finalità:
- Identificazione del cliente per interventi di installazione/assistenza/manutenzione
- Identificazione del cliente per stesura documentazione di progetto/corrispondenza/trasporto

- **Modalità di raccolta dei dati**

La DOCS raccoglie i dati essenzialmente tramite la modulistica in essere e il contatto diretto con il possibile cliente.

Prima di iniziare o proseguire il trattamento dei dati, i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e dei dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'Interessato solo in caso di necessità.

Il trattamento dei dati in oggetto è effettuato unicamente con riferimento a operazioni, nonché con logiche e mediante forme di organizzazione dei dati, strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità.

Fin dove possibile i dati sono raccolti, di regola, presso l'Interessato o, in alternativa presso la sede dell'Organizzazione, mediante comunicazione di dati che avviene, generalmente, direttamente dall'Interessato stesso.

La **DOCS** ha attivo un proprio sito internet (http://www.docsicurezza.it/) che fa uso di *log file,* nei quali vengono conservate informazioni raccolte in maniera automatizzata durante le visite degli utenti.

Le informazioni raccolte possono essere le seguenti:
- indirizzo internet protocol (IP);
- tipo di *browser* e parametri del dispositivo usato per connettersi al sito;
- nome dell'*internet service provider* (ISP);
- data e orario di visita;
- pagina internet di provenienza del visitatore (referral) e di uscita;
- eventualmente il numero di click.

Le suddette informazioni sono trattate in forma automatizzata e raccolte in forma esclusivamente aggregata al fine di verificare il corretto funzionamento del sito e per motivi di sicurezza (ovvero, sono trattate in base ai legittimi interessi del Titolare del trattamento).

A fini di sicurezza (es.: filtri antispam, firewall, rilevazione virus), i dati registrati automaticamente comprendono (come riportato in precedenza) dati personali quali l'indirizzo IP che può essere utilizzato, conformemente alle leggi vigenti in materia, al fine di bloccare tentativi di danneggiamento al sito internet medesimo o di recare danno ad altri utenti, o comunque attività dannose o costituenti reato.

Tali dati non sono mai utilizzati per l'identificazione o la profilazione dell'Interessato, ma solo a fini di tutela del sito internet e dei suoi utenti.

Qualora il sito consenta l'inserimento di commenti, oppure in caso di specifici servizi richiesti dall'utente, il sito rileva automaticamente e registra alcuni dati identificativi dell'Interessato, compreso l'indirizzo e-mail.

Tali dati si intendono volontariamente forniti dall'Interessato al momento della consultazione del sito, della richiesta di informazioni o contatto, nonché di erogazione del servizio.

Consultando il sito, inserendo un commento o altra informazione, l'Interessato:

- accetta espressamente l'Informativa rilasciata agli Interessati ai sensi dell'Articolo 13 del GDPR e disponibile all'indirizzo https://www.docsicurezza.it/privacy-policy/
- acconsente che i contenuti inseriti siano liberamente diffusi anche a terzi.

I dati ricevuti verranno utilizzati esclusivamente per l'erogazione del servizio richiesto e per il solo tempo necessario per la fornitura del servizio.

Le informazioni che gli utenti del sito internet riterranno di rendere pubbliche tramite i servizi e gli strumenti messi a disposizione degli stessi, sono fornite dall'utente consapevolmente e volontariamente, esentando DOCS da qualsiasi responsabilità in merito a eventuali violazioni delle leggi.

Spetta all'utente verificare di avere i permessi per l'immissione di dati personali di terzi o di contenuti tutelati dalle norme nazionali ed internazionali.

In ogni caso i dati rilevati dal sito non sono forniti mai a terzi, per nessuna ragione, a meno che non si tratti di legittima richiesta da parte dell'autorità giudiziaria e nei soli casi previsti dalla normativa applicabile.

Il sito internet di **DOCS** non ha dei collegamenti/rimandi (*link*) con altri siti internet.

- **Cookies**

Per cookies si intende un elemento testuale che viene inserito nel disco fisso di un computer solo in seguito ad autorizzazione. I cookies hanno la funzione di snellire l'analisi del traffico su internet o di segnalare quando un sito specifico viene visitato e consentono alle applicazioni nel web di inviare informazioni a singoli utenti.

Nessun dato degli utenti viene in proposito acquisito dal sito. Non viene fatto uso di *cookies* per la trasmissione di informazioni di carattere personale, né vengono utilizzati i c.d. *cookies* persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

- **Facoltatività del conferimento dei dati**

L'utente, a parte quanto specificato per i dati di navigazione, è libero di fornire i dati personali per richiedere i servizi offerti dalla società. Il loro mancato conferimento può comportare l'impossibilità di ottenere il servizio richiesto.

L'utente considerato minore non deve fornire i dati personali senza il consenso dei genitori.

- **Modalità di conservazione dei dati**

La **DOCS** custodisce i dati in una banca dati elettronica (aggiornata periodicamente) formata da un data base costituito dal programma gestionale ACUT ERP custodito presso la sede di **DOCS**.

Il *software* è conservato presso la sede di **DOCS**.

- **Figure preposte al trattamento dei dati**

Il Titolare è la DOC Service S.r.l., con sede legale in Via L. Mancini, 5 I-20129 Milano (MI) e sede operativa in Via Monfalcone, 39/N I-20092 Cinisello Balsamo (MI).

La **DOCS** ha nominato il proprio Responsabile del trattamento.

L'Organizzazione dichiara che tutte le figure sopra indicate frequentano corsi di aggiornamento in materia di protezione dei dati.

- **Rete informatica**

La **DOCS** ha una rete dati che si compone come descritto nel documento "P-7500.00_B (Procedura) Gestione della documentazione" (§ 3 ¶ 3.6.1.9).

Pertanto, in riferimento al trattamento dei dati con strumenti elettronici, l'Organizzazione utilizza un sistema di autenticazione informatica.

5 INFORMATIVA

La **DOCS** rilascia all'interessato l'Informativa relativa alla raccolta e al trattamento di dati personali. Essa è rilasciata per iscritto o, se richiesto dall'interessato, anche in via orale e, in tal caso, l'Organizzazione si impegna a comprovare con altri mezzi (es.: fotocopia documento di identità) l'identità dell'interessato[4].

La **DOCS** dichiara di aver adottato una Informativa in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, e disponibile all'indirizzo https://www.docsicurezza.it/privacy-policy/.

La **DOCS** dichiara che l'Informativa viene resa:
- **-** preventivamente all'atto della raccolta dei dati presso lo stesso interessato;
- **-** all'atto della registrazione dei dati, se raccolti in altro modo.

L'Informativa contiene:
- l'origine e la tipologia dei dati personali oggetto del trattamento;
- l'identità esatta e tutti i dati di contatto del Titolare del trattamento;
- l'identità esatta e tutti i dati di contatto del Responsabile del trattamento;
- le finalità[5] e le modalità del trattamento;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati (es.: personale somministrato presso la sede di clienti per la gestione badge);
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

[4] *Nota bene: Questo in conformità all'Articolo 12, comma 1, del GDPR.*
[5] *Nota bene: L'Organizzazione invia una nuova Informativa e raccoglie un nuovo consenso nel caso in cui cambino le finalità dei dati.*

- l'indicazione all'interessato del diritto di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- il diritto di proporre reclamo a un'autorità di controllo;
- la specifica e chiara indicazione dei diritti di revoca del consenso, di accesso ai dati, di rettifica, di cancellazione (c.d. diritto all'oblio), di limitazione del trattamento, di portabilità dei dati e di opposizione;
- l'esistenza, qualora presente, di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato;
- la richiesta di consenso.

Se i dati raccolti non vengono forniti direttamente dall'Interessato, l'Informativa indica anche:
- il periodo di conservazione dei dati personali, oppure - se questo non è possibile - i criteri utilizzati per determinare tale periodo;
- la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico. In ogni caso DOCS dichiara di raccogliere i dati solo presso l'interessato.

La **DOCS**, qualora i dati sono raccolti a distanza, si impegna a inviare l'Informativa entro il termine massimo di 1 mese da quando i dati sono stati raccolti o, nel caso in cui i dati vengano raccolti per comunicazioni dirette all'interessato, non oltre la prima comunicazione a questi dei sui dati personali.

La **DOCS** comunque dichiara di essere consapevole quanto sopra non si applica nelle ipotesi in cui[6]:
- l'Interessato dispone già delle informazioni;
- comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie[7] previste, o nella misura in cui l'obbligo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento;
- l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione Europea o dello Stato membro cui è soggetto il Titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'Interessato;
- i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione Europea o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

La **DOCS** non applica la normativa applicabile in oggetto quando:
- il trattamento dei dati deve essere effettuato unicamente nell'ambito dei rapporti intercorrenti tra persone giuridiche, imprese, enti o associazioni;

[6] *Nota bene: Questo in conformità all'Articolo 89, § 1, del GDPR.*
[7] *Nota bene: In tali casi, il Titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.*

- i dati oggetto di trattamento devono essere relativi alla persona giuridica, impresa, ente o associazione;
- il trattamento deve essere effettuato per finalità amministrative o contabili.

La **DOCS** applica la normativa applicabile in oggetto quando:

- il Titolare o l'Interessato del trattamento dei dati sono persone fisiche;
- il Titolare o l'Interessato del trattamento dati sono persone giuridiche, ma fuori dall'ambito delle finalità amministrative o contabili.

6 CONSENSO

La **DOCS** si impegna a non accettare forme di consenso tacito o mediante opzioni già preselezionate.

La **DOCS** si impegna a richiedere nuovo consenso agli Interessati per i dati già raccolti prima dell'entrata in vigore del Regolamento in oggetto, solo se questo tipo di dati non corrispondono alla normativa applicabile precedentemente vigente.

La **DOCS** si impegna a fare in modo che se il consenso dell'Interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

La **DOCS** nel caso di diffusione dei dati a Terzi (es.: consulenti, professionisti con attività in *outsourcing*) per motivi di organizzazione o altri (es.: attività di gestione amministrativa, fiscale o di rapporti economici) non richiede il consenso da parte di coloro cui i dati personali si riferiscono, essendo i Terzi comunque Incaricati al trattamento dei dati, mentre il Titolare del trattamento resta sempre l'Organizzazione che ne effettua la raccolta.

La **DOCS** però si assicura che i Terzi rilascino al Titolare del trattamento, dichiarazione di garanzia di corretta gestione dei dati personali loro affidati, in attuazione delle disposizioni ricevute.

Inoltre, con esclusione della diffusione, il consenso non è richiesto quando il trattamento riguarda la comunicazione di dati tra società, enti o associazioni con società controllanti, controllate o collegate ai sensi dell'art. 2359 del codice civile, ovvero con società sottoposte a comune controllo, nonché tra consorzi, reti di imprese e raggruppamenti e associazioni temporanei di imprese con i soggetti a essi aderenti, per le finalità amministrativo contabili[8] e purché queste finalità siano previste espressamente con determinazione resa agli interessati all'atto dell'Informativa.

7 DIRITTI DELL'INTERESSATO

L'Interessato dal trattamento dei dati ha il diritto di ottenere dal titolare del trattamento:

- **Diritto di accesso dell'interessato**
  la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
  - le finalità del trattamento
  - le categorie di dati personali in questione
  - i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi od organizzazioni internazionali

[8] *Nota bene: Le finalità amministrativo contabili sono definite dall'Articolo 34, comma 1-ter, del GDPR.*

- il periodo di conservazione dei dati personali previsto, quando possibile, oppure, se non è possibile, i criteri utilizzati per determinare tale periodo
- l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento
- il diritto di proporre reclamo a un'autorità di controllo
- tutte le informazioni disponibili sulla loro origine, qualora i dati non siano raccolti presso l'Interessato
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato

- **Diritto di Rettifica**
  L'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo.
  Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
- **Diritto alla cancellazione detto anche "Diritto all'oblio"**
  L'Interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
  - i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati
  - l'interessato revoca il consenso su cui si basa il trattamento[9] e se non sussiste altro fondamento giuridico per il trattamento
  - l'interessato si oppone al trattamento[10] e non sussiste alcun motivo legittimo prevalente per procedere al trattamento
  - i dati personali sono stati trattati illecitamente
  - i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento
  - i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione[11]
- **Diritto di limitazione del Trattamento**
  L'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
  - l'Interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali
  - il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo
  - benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

---

[9] *Nota bene: La revoca avviene conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), del GDPR.*
[10] *Nota bene: L'opposizione avviene ai sensi dell'articolo 21, paragrafo 1 e 2, del GDPR.*
[11] *Nota bene: società dell'informazione definite all'articolo 8, paragrafo 1, del GDPR.*

– l'Interessato si è opposto al trattamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'Interessato.

La **DOCS**, al fine di rendere più trasparente la propria condotta in tema di raccolta e trattamento dei dati e di agevolare l'Interessato nell'esercizio della tutela dei propri diritti, allega al presente documento i facsimili dei documenti utili all'esercizio dei propri diritti da parte dell'Interessato.

8 PROCEDURE DI SICUREZZA E VERIFICA DI TENUTA DEL SISTEMA INFORMATICO

8.1 SISTEMA DI AUTENTICAZIONE INFORMATICA

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono in un *user* per l'identificazione dell'incaricato associata ad una *password* riservata, conosciuta solamente dal medesimo e dal Responsabile al trattamento dei dati.

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

Lo user è univoco, laddove utilizzata, non viene assegnata ad altri incaricati, neppure in tempi diversi.

Le credenziali di autenticazione (user e password) sono disattivate e cancellate in caso di cessazione del rapporto di lavoro tra **DOCS** e l'incaricato.

Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

La **DOCS** dichiara che gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente.

La **DOCS** garantisce che il *back up* dei dati è eseguito secondo le modalità descritte all'interno del documento "P-7500.00_B (Procedura) Gestione della documentazione" (§ 3 ¶ 3.6.1.10).

Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

8.2 SISTEMA DI AUTORIZZAZIONE

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

8.3 Eventuali Trattamenti senza l'ausilio di strumenti elettronici

La **DOCS**, in caso di trattamenti senza l'ausilio di strumenti elettronici, dichiara che agli incaricati sono impartite istruzioni scritte finalizzate al controllo e alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale e relativo all'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati è redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

Quando gli atti e i documenti contenenti dati personali sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

La **DOCS** dichiara che l'accesso agli eventuali archivi contenenti dati sensibili è controllato.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Per gli archivi cartacei, e quindi non dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

La **DOCS**, nei rapporti con i Clienti e i Fornitori, ritiene data l'Informativa al momento dell'avvio di rapporti commerciali.

L'Informativa al personale (es.: collaboratori, dipendenti), contiene i necessari riferimenti al trattamento dei dati sensibili, delle limitazioni e garanzie fornite per il trattamento di tali dati e quant'altro necessario derivante da motivazioni legittime e sostenibili, con comunicazione del Titolare del trattamento dei dati e dell'eventuale Terzo incaricato (vedere anche precedente § 6 CONSENSO).

8.4 DATA BREACH

La **DOCS** si impegna a notificare alla Autorità di Controllo le violazioni di dati personali di cui venga a conoscenza senza ingiustificato ritardo e comunque (e se possibile) entro 72 ore dal momento in cui sia venuta a conoscenza della violazione.

La **DOCS** riconosce che nel caso in cui la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, deve comunicare all'interessato la violazione senza ritardo e con un linguaggio semplice e chiaro.

La **DOCS** si impegna a notificare le informazioni richieste dal GDPR quali, ad esempio, la descrizione della natura della violazione e, se possibile, il numero degli interessati, le probabili conseguenze della violazione, la descrizione delle misure adottate o da adottare per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

La **DOCS** si impegna in caso di notifica effettuata con ritardo ad indicare i motivi del ritardo. Nel caso in cui la violazione rappresenti un rischio elevato per i diritti e le libertà dell'interessato, l'Organizzazione si impegna a darne comunicazione, senza ritardo, direttamente allo stesso interessato.

La **DOCS** però avverte che la comunicazione all'interessato non è richiesta se:

a) il titolare del trattamento ha messo in atto misure tecniche e organizzative adeguate di protezione applicate ai dati oggetto di violazione, in particolare quelle destinate a rendere i dati personali incomprensibili ai non autorizzati, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un "rischio elevato" per i diritti e le libertà degli interessati;
c) se la comunicazione richiederebbe "sforzi spropositati"; in tal caso si procede a una comunicazione pubblica.

La **DOCS** si impegna a tenere nota di tutte le eventuali violazioni, anche non subordinate ad obbligo di notifica al Garante

8.5 REGISTRO DEL TRATTAMENTO DATI

La **DOCS** dichiara, ai sensi dei requisiti contenuti nel GDPR, di non essere soggetto obbligato alla tenuta del registro del Trattamento dei dati.

9 ALLEGATI

1) Fac simile Informativa;
2) Fac simile consenso al trattamento dati;
3) Fac simile domanda esercizio dei diritti dell'Interessato;
4) Fac simile di reclamo al Garante per l'Interessato.

I suddetti allegati sono disponibili per consultazione c/o la sede di DOCS e possono essere inviati all'Interessato a seguito di specifica richiesta all'indirizzo e-mail privacy@docsicurezza.it.