ARBONIA

Direttiva relativa al trattamento dei dati (Direttiva sulla privacy)

16 giugno 2020

ARBONIA

INDICE

ARBONIA

1 SCOPO E FINALITÀ

Per adempiere agli obblighi normativi e contrattuali assunti è indispensabile procedere alla raccolta e al trattamento di dati di natura personale. Nel compiere tali operazioni è obbligatorio ottemperare alle normative sulla privacy vigenti nel singolo paese. La presente direttiva illustra le modalità con le quali Arbonia AG e le società ad essa consociate (di seguito denominate "Arbonia" o "Società del Gruppo") trattano i dati personali. Le disposizioni qui riportate valgono come standard minimo. In presenta di normative locali più stringenti in materia di privacy, è richiesto il rispetto di queste ultime. Devono essere rispettate anche eventuali disposizioni locali che disciplinano l'attuazione della presente direttiva.

La presente direttiva relativa al trattamento dei dati ("Direttiva sulla privacy") ha come obiettivi la definizione, l'implementazione, il rispetto e il miglioramento continuo della tutela dei dati personali, in ottemperanza ai requisiti del Regolamento Generale sulla protezione dei dati dell'Unione Europea 2016/679 (GDPR) e a tutte le leggi sulla privacy localmente vigenti (**leggi applicabili in materia di protezione dei dati**) da parte di Arbonia.

Il mancato rispetto delle leggi applicabili in materia di protezione dei dati espone Arbonia al pericolo di danni alla reputazione e sanzioni penali pesanti (ad esempio fino al 4% del fatturato mondiale ai sensi del GDPR), e i nostri clienti e collaboratori a specifici rischi inerenti la protezione dei dati, come ad esempio, furti di identità o perdite finanziarie. Il rispetto delle leggi applicabili in materia di protezione dei dati contribuisce a mantenere la fiducia nell'organizzazione di Arbonia e a garantire la corretta operatività dell'azienda.

La finalità della presente Direttiva sulla privacy è quella di fornire un quadro di riferimento per soddisfare i requisiti di tutela dei dati personali all'interno di Arbonia, puntando, in particolare, a implementare i principi fondamentali per il trattamento dei dati personali (**principi di protezione dei dati**), illustrati nel paragrafo 6, la cui responsabilità spetta alle società di Arbonia, nella misura in cui esse agiscono quali "Titolari del trattamento" ai sensi del GDPR; essa disciplina inoltre la necessità di misure tecniche ed organizzative adeguate e le segnalazioni di incidenti a danno della privacy come standard minimo per tutte le società di Arbonia ed è valida per tutti i dipendenti di Arbonia e per i membri del consiglio d'amministrazione di Arbonia AG.

L'informativa fornisce infine un quadro di riferimento per ulteriori requisiti, applicabile ai titolari e ai responsabili del trattamento ai sensi del GDPR (o leggi sulla privacy analogamente applicabili), come descritto nel paragrafo 7.

2 TERMINI E DEFINIZIONI

Ai fini della presente Direttiva sulla privacy valgono i seguenti termini e definizioni:

"Dati anonimizzati": indica l'impossibilità che qualcuno risalga a una determinata identità da detti dati o il fatto che risalire a detta identità personale richiederebbe uno sforzo sproporzionato in termini di tempo, costi e lavoro.

"Leggi applicabili in materia di protezione dei dati": il Regolamento generale sulla protezione dei dati dell'Unione Europea 2016/679 (**GDPR**) o tutte le altre leggi nazionali applicabili in materia di protezione dei dati che includono disposizioni analoghe.

"Responsabile dei processi aziendali": ai fini della presente Direttiva sulla privacy, la persona fisica responsabile delle singole applicazioni IT.

"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;

"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;

"**Incidente a danno della privacy"**: qualsiasi evento che dà adito a un sospetto fondato di acquisizione, raccolta, modifica, copia, trasmissione e alterazione di dati personali in violazione delle leggi applicabili. Può riferirsi ad azioni di terzi o di collaboratori.

"Interessato": qualsiasi persona fisica identificata o identificabile. 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.

"**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;

"**Registri delle attività di trattamento":** tutte le registrazioni dei trattamenti mantenute sotto la responsabilità del titolare del trattamento. Tale registro contiene tutte le seguenti informazioni: (i) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del coordinatore locale della protezione dei dati; (ii) le finalità del trattamento; (iii) una descrizione delle categorie degli interessati e delle categorie di dati personali; (iv) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari in

paesi terzi; (v) ove applicabile, i trasferimenti di dati personali verso un paese terzo, compresa l'identificazione del paese terzo e la documentazione delle garanzie adeguate; (vi) i termini ultimi previsti per la cancellazione delle diverse categorie di dati; (vii) una descrizione generale delle misure di sicurezza tecniche e organizzative.

"**Garante della privacy o coordinatore della protezione dei dati**": la persona descritta nel paragrafo 5.

"**Dati personali**": qualsiasi informazione riguardante l'interessato (inclusi i dati personali relativi a categorie speciali), ovvero a una persona fisica identificata o identificabile, come, ad esempio, il nome, la data di nascita, l'indirizzo e-mail, la religione, i dati relativi all'ubicazione, i dati online (indirizzo IP, dati di localizzazione, ecc.), codici (numero di previdenza sociale, numero del documento d'identità , ecc.), caratteristiche fisiche (sesso, colore della pelle, dei capelli e degli occhi, ecc.), dati cliente e molto altro) disciplinate da uno dei regolamenti sulla privacy vigenti.

"**Trattamento**" o "**Trattare**": 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;

"**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;

"Categorie particolari di dati personali": dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, le condanne penali pregresse, l'appartenenza sindacale, le condizioni di salute e l'orientamento sessuale dell'interessato, nonché i dati genetici e biometrici, con l'obiettivo di identificare in modo univoco una persona fisica.

"Paesi terzi": le nazioni che non sono Stati membri dell'Unione Europea o dello Spazio Economico Europeo o paesi con un livello di protezione dei dati ritenuto adeguato dalla Commissione Europea (cfr. elenco dei paesi con livello di protezione dei dati adeguato: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

"Terzi": qualsiasi persona diversa dall'interessato, dal titolare del trattamento o dal responsabile del trattamento (inclusi eventuali partner commerciali, sub-contraenti, agenzie di rating e altri), nonché persone autorizzate per autorità diretta del titolare del trattamento

o del responsabile del trattamento a trattare i dati personali. In caso di trattamento dei dati personali in virtù di un'autorizzazione, i responsabili del trattamento non sono considerati terzi ai sensi della legge sulla protezione dei dati, in quanto giuridicamente assimilati ai titolare del trattamento.

3 AMBITO D'APPLICAZIONE

3.1 Ambito d'applicazione a livello di organizzazione

La presente Direttiva sulla privacy vale per tutte le società del gruppo Arbonia, per tutti i dipendenti di Arbonia e per i membri del consiglio d'amministrazione di Arbonia AG. L'implementazione della direttiva è obbligatoria per legge in ogni società del gruppo.

3.2 Leggi, regolamenti, standard e direttive

La presente Direttiva sulla privacy recepisce tutti i requisiti del GDPR e i principi di protezione dei dati riconosciuti a livello internazionale, senza sostituire, ma andando ad integrare, il diritto nazionale in materia. Quest'ultimo mantiene comunque la priorità in caso di conflitti con la presente Direttiva sulla privacy o in caso di requisiti più stringenti rispetto a quelli in essa stabiliti. I contenuti della presente Direttiva sulla privacy devono essere tenuti in considerazione anche in assenza di una legislazione nazionale in materia.

Qualora la presente Direttiva sulla privacy entri in contraddizione con le disposizioni applicabili in un determinato paese, sarà possibile recepire le disposizioni specifiche della presente Direttiva sulla privacy in accordo con Head Legal & Compliance redigendo un'apposita direttiva a valenza locale. I contenuti e la finalità di base delle disposizioni interessate non possono però essere modificate.

4 FONDAMENTO NORMATIVO

La presente Direttiva sulla privacy si basa sul GDPR e sui principi di protezione dei dati globalmente accettati.

5 RUOLI E COMPETENZE

- L'amministratore di una società del gruppo[1] è responsabile di:
  1. garantire in ultima istanza che la persona giuridica in questione soddisfi i rispettivi obblighi di legge in materia di trattamento dei dati personali;
  2. garantire che i requisiti della presente Direttiva sulla privacy vengano soddisfatti (compresa la segnalazione degli incidenti a danno della sicurezza dei dati).
  3. garantire che il responsabile dei processi aziendali compili e tenga aggiornati i "registri delle attività di trattamento" a livello di società del gruppo;
  4. nominare una persona formalmente incaricata della protezione dei dati a livello locale (interna o esterna) (di seguito denominato "garante della privacy"), se ciò è richiesto dal regolamento sulla privacy localmente vigente, dando comunicazione della persona designata a Head Legal & Compliance entro la metà di ogni anno;
  5. nominare un responsabile della protezione dei dati locale (di seguito denominato "coordinatore della protezione dei dati"), se il regolamento sulla privacy localmente applicabile non prevede l'istituzione di un garante della privacy locale. La persona nominata deve essere comunicata a Head Legal & Compliance e Internal Audit entro la metà di ogni anno.

- Il coordinatore della protezione dei dati e/o garante della privacy incaricati dall'amministratore di una società del gruppo [2] deve:
  1. monitorare il rispetto della presente Direttiva sulla privacy e delle direttive impartite dal titolare del trattamento o dal responsabile del trattamento in riferimento alla tutela dei dati personali, ivi compresi il trasferimento delle competenze e i relativi controlli;
  2. fornire informazioni e consulenza e controllare che il titolare del trattamento o il responsabile del trattamento ottemperino agli obblighi di trattamento di cui alla presente Direttiva sulla privacy;
  3. se richiesti, fornire suggerimenti per un'eventuale valutazione d'impatto sulla protezione dei dati e monitorarne i risultati, oltre a rispondere ad eventuali altre domande sui dati personali che potrebbero essergli rivolte nell'ambito della presente Direttiva sulla privacy;
  4. tenere aggiornati i "registri delle attività di trattamento" compilati dalla singola società del gruppo nella persona del responsabile dei processi aziendali, e

[1] Per le società del gruppo non operative questa competenza viene definita in separata sede in accordo con Head Legal & Compliance.
[2] Per le società del gruppo non operative questa competenza viene definita in separata sede in accordo con Head Legal & Compliance.

confermarne la completezza e l'attualità a Head Legal & Compliance entro la metà di ogni anno.
5. fungere da punto di contatto di Head Legal & Compliance e tenerli informati su responsabilità, rischi e problemi concernenti la tutela dei dati personali;
6. supportare il team IT responsabile dell'applicazione IT nelle attività di controllo e autorizzazione di nuove applicazioni IT a livello di società del gruppo per il trattamento di dati personali e di ogni applicazione IT per il trattamento di categorie particolari di dati personali in ottica di privacy;
7. autorizzare la trasmissione di dati personali in un paese terzo in ottica di protezione dei dati (cfr. n. 14 infra).
8. fungere da sportello locale dell'autorità di controllo per eventuali domande riguardanti il trattamento dei dati, e collaborare con detta autorità di controllo;
9. gestire richieste di informazioni di dipendenti coinvolti nel trattamento di dati personali;
10. gestire richieste di informazioni di interessati in merito ai dati personali di loro proprietà detenuti da Arbonia, oppure in caso di richiesta di informazioni da parte di più società del gruppo, trattare tale evenienza in collaborazione con Corporate IT (cfr. anche n. 7.4) infra;
11. verificare e autorizzare i contratti o gli accordi perfezionati e/o pre-esaminati dal responsabile dei progetti aziendali con i responsabili del trattamento autorizzati a gestire i dati personali per conto di Arbonia come descritto al paragrafo 7.2;
12. supervisionare i garanti della privacy locali eventualmente assunti esternamente per tale incarico;
13. segnalare eventuali incidenti inerenti la sicurezza dei dati ai sensi della direttiva Data Breach Notification (cfr. n. 9 infra e la "Arbonia Data Breach Policy").

- La commissione IT in collaborazione con Corporate IT è responsabile di:
  1. definire gli standard validi a livello di gruppo e i controlli IT generali (GITC, General IT Controls) da tenere in considerazione per l'archiviazione dei dati;

- I team IT delle singole società del gruppo sono responsabili di:
  1. garantire attraverso appositi standard, policy e l'esecuzione dei controlli IT generali (GITC), che i sistemi, i servizi e le infrastrutture utilizzati per l'archiviazione dei dati soddisfino standard di sicurezza accettabili (controlli degli accessi/cancellazione dei dati), tenendo altresì 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;
  2. prodigarsi affinché il titolare e il responsabile del trattamento mettano in atto misure tecniche e organizzative opportune per garantire un livello di sicurezza adeguato al rischio, come indicato nel paragrafo 8;
  3. previa consultazione con il coordinatore della protezione dei dati e/o con il garante della privacy, verificare e autorizzare nuove applicazioni IT per il trattamento dei dati personali in ottica di tutela della privacy;

4. eseguire verifiche e controlli regolari per assicurare che i componenti hardware e software rilevanti per la sicurezza funzionino correttamente; i risultati dei controlli di sicurezza devono essere comunicati al garante della privacy competente.
5. valutare la sicurezza dei dati di tutti i servizi terzi (ad es. responsabile del trattamento) che chiamano in causa la società per il trattamento di dati personali (servizi di cloud computing, ecc.);
6. mantenere un elenco degli incidenti a danno della privacy e segnalare eventuali incidenti inerenti la sicurezza dei dati a Corporate IT;
7. coordinare e rispondere alle richieste di informazioni presentate dagli interessati in merito ai dati personali di loro proprietà detenuti dalla società di Arbonia che si avvale del servizio di consulenza IT (cfr. anche il n. 7.4) infra;
8. segnalare gli incidenti o rischi inerenti la sicurezza dei dati eventualmente rilevati, come indicato nella direttiva Data Breach Notification (cfr. n. 9 infra e la "Arbonia Data Breach Policy")

- Corporate IT, in collaborazione con il team IT incaricato dell'assistenza alla società del gruppo interessata, è responsabile di:
  1. eseguire verifiche e controlli regolari per assicurare che i componenti hardware e software rilevanti per la sicurezza funzionino correttamente; i risultati dei controlli di sicurezza devono essere comunicati al garante della privacy competente.
  2. mantenere un elenco degli incidenti a danno della privacy;
  3. segnalare gli incidenti o rischi inerenti la sicurezza dei dati eventualmente rilevati, come indicato nella direttiva Data Breach Notification (cfr. n. 9 infra e la "Arbonia Data Breach Policy").

- Internal Audit è responsabile di:
  1. verificare con una prova basata sul rischio condotta contestualmente agli audit effettuati secondo il regolare piano di audit, se i processi organizzativi soddisfano le disposizioni essenziali della presente Direttiva sulla privacy;

- Il responsabile dei processi aziendali è responsabile di:
  1. garantire che il garante della privacy locale venga interpellato adeguatamente e tempestivamente in tutte le questioni necessarie per valutare il trattamento dei dati personali;
  2. perfezionare e/o pre-esaminare con il responsabile del trattamento tutti i contratti o gli accordi che possono includere un trattamento di dati personali, come descritto al paragrafo 7.2;
  3. compilare e tenere aggiornati i "registri delle attività di trattamento" mantenuti dalla singola società del gruppo, e confermare al coordinatore della protezione dei dati e/o al garante della privacy entro fine aprile di ogni anno l'integrità e l'attualità delle registrazioni;
  4. prima dell'implementazione di nuovi processi di elaborazione dei dati personali, stimare i rischi risultanti per l'identità personale e i diritti fondamentali degli interessati, e qualora questa violazione dei dati personali sia suscettibile di

presentare un rischio elevato per i diritti e le libertà dell'interessato eseguire preventivamente una valutazione d'impatto sulla protezione dei dati;

6 PRINCIPI DI PROTEZIONE DEI DATI PER IL TRATTAMENTO DI DATI PERSONALI

Ogni società del gruppo coinvolta nel trattamento di dati personali in qualità di titolare del trattamento, deve assicurare la dimostrabilità del rispetto dei **6 (sei) principi fondamentali per il trattamento dei dati personali** riportati di seguito:

1. Trattare i dati personali esclusivamente in presenza di una base giuridica valida e comprovabile ai sensi delle leggi applicabili in materia di dati personali, e solo se l'interessato è informato in merito all'identità, ai dati di contatto del titolare del trattamento, alle modalità e alle basi giuridiche dei dati personali rilevati, ai termini di conservazione e alle finalità per le quali i dati personali vengono raccolti.

2. Tenere sempre in considerazione lo scopo per il quale i dati personali vengono raccolti.

3. Raccogliere/trattare solo i dati personali strettamente necessari.

4. Conservare i dati personali in modo corretto ed eliminare i dati personali errati.

5. Conservare i dati personali solo per i periodi stabiliti per legge.

6. Trattare con riservatezza i dati personali e divulgare solo i contenuti strettamente necessari.

6.1 Correttezza, legittimità e trasparenza

I dati personali possono essere trattati solo per gli scopi consentiti descritti nel prosieguo; il trattamento deve avvenire secondo il principio della trasparenza. Qualsiasi trattamento di dati personali deve pertanto essere lecito e corretto, e deve avvenire nel rispetto dei diritti individuali degli interessati. Esso può riferirsi a dati che Arbonia ottiene direttamente dall'interessato (ad esempio tramite la compilazione di moduli o tramite la corrispondenza a mezzo posta ordinaria, telefono, posta elettronica o altro), o a dati pervenuti ad Arbonia da terzi.

Ai sensi delle leggi applicabili in materia di protezione dei dati è consentito il trattamento di dati personali giuridicamente fondati su uno dei **cinque motivi legittimi** (**motivi legittimi**) stabiliti dal GDPR. Detti motivi sono:

1. **Contratto:** il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, oppure

2. **Consenso:** il trattamento dei dati personali si basa sul consenso dell'interessato (modello Opt-in) in merito a uno o più scopi specifici. Il consenso deve essere documentato, oppure

3. **Obbligo legale:** il trattamento dei dati personali si basa su un obbligo legale a carico di Arbonia. La natura e l'oggetto del trattamento dei dati devono essere necessari per l'attività di trattamento consentita dalla legge e devono soddisfare le condizioni legali, oppure

4. **Pubblico interesse:** il trattamento è richiesto per l'esecuzione di un compito svolto nel pubblico interesse, oppure

5. **Interessi commerciali legittimi:** il trattamento risponde ragionevolmente ad interessi commerciali legittimi di Arbonia o di terzi ai quali i dati personali vengono comunicati, salvo ove gli interessi o i principi e le libertà fondamentali dell'interessato prevalgano su detti interessi commerciali. I legittimi interessi sono generalmente di natura giuridica (ad es. rivendicazione di richieste pendenti / tramite accordi tariffari con il comitato aziendale / accertamento / esercizio / difesa di un diritto in sede giudiziaria nei confronti dell'interessato) o commerciale (tentativo di evitare violazioni del contratto).

Il principio della trasparenza impone che l'interessato venga informato sulle modalità con cui i suoi dati personali vengono trattati. In linea generale, è quindi consigliabile ottenere i dati personali direttamente dall'interessato (e non attraverso terzi). Se devono essere trattati dati personali, l'interessato deve essere informato in merito a:

- i nomi e i dati di contatto del titolare del trattamento ed, eventualmente, del relativo rappresentante in sede europea
- se applicabile, i dati di contatto del coordinatore della protezione dei dati e/o garante della privacy
- lo scopo e la base giuridica del trattamento dei dati personali
- i destinatari terzi o le categorie di destinatari terzi ai quali i dati possono essere trasmessi
- se applicabile, informazioni sul trattamento in un paese terzo con indicazione delle garanzie adeguate

6.2 Limitazione della finalità

I dati personali possono essere trattati solo per lo scopo comunicato all'interessato prima dell'acquisizione dei dati stessi. Eventuali modifiche successive della finalità sono ammesse in

misura limitata e richiedono una motivazione. Il titolare del trattamento deve informare l'interessato sulla finalità per la quale Arbonia tratta i suoi dati personali, la prima volta che la società rileva i dati dell'interessato o non appena possibile. Ad ogni trattamento per finalità pubblicitarie o di marketing, all'interessato deve essere concesso un diritto di opposizione, in merito al quale l'interessato deve essere espressamente informato. A tale riguardo ogni titolare del trattamento deve attuare una gestione dei reclami che garantisca il rispetto di eventuali Opt-Out.

6.3 Minimizzazione dei dati

Devono essere raccolti/trattati solo i dati personali strettamente necessari. Prima del trattamento dei dati personali occorre stabilire se e in che misura detto trattamento è o meno necessario per raggiungere la finalità per la quale viene effettuato. Non è consentito raccogliere dati personali in maniera preventiva, né conservarli per possibili scopi futuri, salvo ove sia imposto o ammesso dalle leggi nazionali applicabili.

6.4 Dati esatti e aggiornati

I dati personali devono essere esatti, completi e, qualora intervengano modifiche, mantenuti aggiornati. Devono essere intraprese misure opportune a garantire che eventuali dati personali inesatti o incompleti vengano eliminati, corretti, integrati o aggiornati. Tutti coloro che maneggiano dati personali devono attuare le opportune misure (ad esempio richiedendo conferma dei dati personali all'interessato quando questi telefona, oppure eliminando un numero di telefono salvato in rubrica se l'interessato non utilizza più tale numero).

6.5 Termini di conservazione limitati

I dati personali devono essere conservati solo per il periodo effettivamente necessario. I dati personali devono essere cancellati, non appena non più necessari per gli scopi previsti oppure non appena viene revocato il consenso o viene meno il legittimo interesse per il quale vengono utilizzati, e Arbonia non può addurre motivi legittimi prevalenti. In alcuni casi, termini di conservazione prolungati possono autorizzarci a conservare i dati personali più a lungo, se ciò è richiesto per legge (ad es. in ottemperanza al diritto commerciale e tributario), o se i dati personali sono necessari per l'accertamento, l'esercizio e la difesa di un diritto in sede giudiziale.

6.6 Riservatezza e sicurezza dei dati

I dati personali devono essere trattati con riservatezza e divulgati solo se strettamente necessario. Vale il principio di "informazione necessaria", tale che dipendenti e terzi possono ottenere l'accesso ai dati personali solo se e nella misura in cui tale accesso è finalizzato al raggiungimento della finalità dichiarata. Ciò esige la presenza di un concetto accuratamente sviluppato a definire i diritti di accesso specifici per ciascun processo aziendale e la relativa implementazione, inclusi i ruoli e le competenze (concetto dei diritti di accesso). I destinatari di dati personali devono essere informati in merito alla riservatezza dei dati personali **e**

devono assoggettarsi a un accordo di riservatezza/non divulgazione (che può essere parte del contratto di lavoro o strumento analogo). Eccezione: il destinatario è soggetto a un obbligo di non divulgazione per legge o giusto accordo professionale.

I dati personali devono essere protetti mediante misure tecniche ed organizzative adeguate, in modo da evitare ogni possibile accesso o divulgazione non autorizzati, ed eventuali perdite, modifiche o distruzioni accidentali (cfr. paragrafo 8).

7 ALTRI OBBLIGHI AI SENSI DEL GDPR O ALTRE NORMATIVE APPLICABILI IN MATERIA DI PROTEZIONE DEI DATI

7.1 Principio di responsabilizzazione

Qualsiasi società del gruppo Arbonia soggetta al GDPR (o ad analoga normativa in materia di protezione dei dati) deve garantire la dimostrabilità del rispetto delle leggi applicabili in materia di protezione dei dati (principio di "responsabilizzazione"). Pertanto, in aggiunta ai requisiti generali previsti nella presente Direttiva sulla privacy, le società del gruppo sono tenute ad implementare e rispettare i punti riportati di seguito; nella fattispecie, spetta all'amministratore della società del gruppo di volta in volta interessata, assicurare che gli stessi vengano effettivamente implementati e mantenuti.

1. Coordinatore della protezione dei dati e/o garante della privacy locale: nomina di un coordinatore della protezione dei dati e/o garante della privacy locale specifico

2. Tenuta dei "registri delle attività di trattamento": deve essere compilato e mantenuto aggiornato un inventario delle attività di trattamento dei dati personali

3. Controllo di legittimità: è necessario verificare che il trattamento dei dati personali avvenga in modo conforme alla legge nel rispetto dei motivi legittimi, in particolare se il trattamento coinvolge categorie particolari di dati personali

4. Controllo del responsabile del trattamento: conclusione di un contratto di nomina a responsabile del trattamento dei dati personali con il soggetto al quale viene affidato tale ruolo o in qualità di responsabile del trattamento in caso di fornitura o ricezione di dati personali in virtù di un'autorizzazione di cui all'art. 28 GDPR.

5. In caso di contitolari del trattamento è necessario prevedere un accordo tra i contitolari come da art. 26 GDPR.

6. I dipendenti di Arbonia devono essere informati sulle attività di trattamento dei dati personali.

7.2 Regole per i responsabili del trattamento (in particolare partner di servizio)

Il titolare del trattamento ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti dell'articolo 28 GDPR e garantisca la tutela dei diritti dell'interessato.

Per i servizi condivisi internamente ad Arbonia è previsto un accordo che consente di trasmettere i dati personali, purché sussistano motivi legittimi per la trasmissione di detti dati personali in conformità alle leggi applicabili in materia di protezione dei dati.

7.2.1 Fornitura dei dati personali al responsabile del trattamento (in uscita)

Il trattamento dei dati personali in virtù di un'autorizzazione determina la situazione per cui un fornitore di servizi viene incaricato di trattare i dati personali senza accollo della responsabilità del processo aziendale corrispondente (ad es. fornitori di servizi, servizi in outsourcing, ecc.). In casi come questi è necessario stipulare un contratto di nomina a responsabile del trattamento dei dati personali in virtù di un'autorizzazione con vendor esterni. La società del gruppo Arbonia in questione detiene il ruolo di titolare del trattamento e mantiene la completa responsabilità della corretta esecuzione del trattamento dei dati personali ad opera del responsabile del trattamento.

Il responsabile dei processi aziendali interessato deve garantire che per conferire l'incarico a tali fornitori di servizi venga utilizzato l'accordo quadro aggiornato per la nomina a responsabile del trattamento dei dati personali o un accordo equivalente messo a disposizione dal fornitore di servizi, onde soddisfare i requisiti dell'articolo 28 GDPR. In alternativa il fornitore di servizi può documentare l'avvenuto rispetto da parte sua dei requisiti per la sicurezza dei dati presentando un'idonea certificazione UE debitamente autorizzata. Qualsiasi deviazione da tale standard deve essere approvata dal garante della privacy e/o coordinatore della protezione dei dati in collaborazione con Corporate IT. I contratti esistenti devono essere revisionati entro un anno dall'entrata in vigore della presente Direttiva sulla privacy e devono includere un accordo di nomina a responsabile del trattamento.

7.2.2 Ricezione di dati personali in qualità di responsabile del trattamento (in entrata)

Se vengono trasmessi dati personali da un terzo a una società del gruppo Arbonia, è necessario garantire che i dati personali (i) possano essere utilizzati per la finalità prevista, (ii) vengano rilevati in virtù di motivi legittimi (si consiglia di richiedere una conferma scritta) e (iii) sia presente un contratto di nomina a responsabile del trattamento come da articolo 28 GDPR.

7.3 Trasmissione transfrontaliera di dati personali

In caso di trasmissione transfrontaliera di dati personali devono essere soddisfatti i requisiti nazionali per la divulgazione dei dati personali all'estero. Ai sensi del GDPR è consentito il trasferimento di dati personali all'interno dell'UE, del SEE o verso un paese per il quale la Commissione Europea ha appurato esistere adeguate garanzie tali da garantire un livello idoneo di sicurezza dei dati. Per un trasferimento di dati di questa natura non è richiesta alcuna autorizzazione. La Commissione Europea ha inserito la Svizzera tra i paesi che offrono un livello adeguato di sicurezza (cfr. elenco dei paesi aggiornato:
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Il trasferimento di dati personali a un paese terzo è consentito solo in presenza di ulteriori garanzie adeguate. Ciò significa che, se il destinatario può dimostrare di adottare uno standard in materia di protezione dei dati equivalente alla presente Direttiva sulla privacy, (ad es. i) sono in atto norme vincolanti d'impresa, ii) sono state concordate clausole contrattuali UE per la designazione dei responsabili del trattamento in paesi terzi con il fornitore del servizio e altre ditte sub-appaltatrici[3], iii) è in atto un codice di condotta redatto dall'autorità di controllo competente, iv) il fornitore aderisce a un sistema di certificazione accreditato dall'UE per il raggiungimento di un livello adeguato di sicurezza dei dati oppure v) sono in atto accordi individuali tra il titolare del trattamento e il responsabile del trattamento in virtù dell'autorizzazione dell'autorità di controllo competente) e avendone informato l'interessato. Tale obbligo non vale se la trasmissione si basa su un obbligo legale. Un trasferimento di tale natura richiede l'autorizzazione del coordinatore della protezione dei dati e/o del garante della privacy.

Se vengono trasmessi dati personali all'interno di Arbonia, la società del gruppo che importa i dati personali è tenuta a collaborare in tutte le richieste di informazioni avanzate dall'autorità di controllo competente nel paese nel quale ha la propria sede legale la società del gruppo che esporta i dati personali, dovendo altresì rispondere a tutte le osservazioni che l'autorità competente possa eventualmente presentare in merito al trattamento dei dati personali.

7.4 Gestione di una richiesta di informazioni ad opera di un interessato

Gli interessati hanno il diritto di presentare una richiesta formale di informazioni sui dettagli dei dati personali detenuti da Arbonia, potendo esercitare i seguenti diritti:

Diritto di ottenere informazioni riguardanti:

- le finalità del trattamento;

[3] Cfr. Decisione della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali standard tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

- le categorie dei dati personali che vengono trattati;
- i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- quando possibile, il periodo di conservazione dei dati personali previsto 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;
- qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione;
- Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate.

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 mediante dichiarazione integrativa.

Diritto alla cancellazione ("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 seguenti motivi:
    1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
    2. l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a) GDPR, o all'articolo 9, paragrafo 2, lettera a) GDPR, e se non sussiste altro fondamento giuridico per il trattamento;
    3. l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1 GDPR, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2 GDPR;
    4. i dati personali sono stati trattati illecitamente;
    5. i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dello Stato membro cui è soggetto il titolare del trattamento;
    6. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1 GDPR;

Diritto di limitazione di trattamento:

- L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre uno dei seguenti presupposti:
- 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;
- l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

L'interessato deve essere invitato a presentare la propria richiesta in forma scritta, per e-mail o per posta, all'indirizzo del garante della privacy locale competente. Le informazioni devono essere fornite all'interessato dal responsabile della protezione dei dati locale senza ingiustificato ritardo, ma in ogni caso entro un mese dalla ricezione della richiesta; detto termine può essere prorogato di ulteriori due mesi se ciò è ritenuto necessario in considerazione della complessità e del numero di richieste. Il coordinatore della protezione dei dati e/o garante della privacy del titolare del trattamento informa l'interessato entro un mese dalla ricezione della richiesta in merito a una proroga del termine, indicandone anche le motivazioni. Per l'interessato non devono insorgere costi per la richiesta di informazioni che lo riguardano detenute da una società del gruppo Arbonia, salvo il caso in cui le richieste avanzate dall'interessato non siano palesemente immotivate o eccessive, specialmente in caso di presentazione reiterata. Le richieste di informazioni presentate da un interessato a più società del gruppo Arbonia devono essere inoltrate a Corporate IT affinché possano essere gestite ed evase in modo coordinato.

7.5 Esecuzione della valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Prima dell'implementazione di nuovi processi di elaborazione dei dati personali devono essere pertanto valutati i rischi risultanti per l'identità personale e i diritti fondamentali dell'interessato. In caso di nuove applicazioni IT se ne dovrà tenere conto nell'ambito della procedura di autorizzazione. Se da una prima disamina emerge che un nuovo tipo programmato di trattamento dei dati personali è suscettibile di presentare un rischio elevato per l'interessato, occorre eseguire una valutazione d'impatto sulla protezione dei dati.

Eventuali richieste di informazioni sulla necessità del trattamento o durante l'esecuzione di una valutazione d'impatto sulla protezione dei dati devono essere indirizzate al coordinatore della protezione dei dati e/o al garante della privacy locale. Dopo l'esecuzione, la valutazione d'impatto sulla protezione dei dati deve essere resa nota al coordinatore della protezione dei dati e/o al garante della privacy locale che deve esprimere la propria posizione a riguardo.

Se dalla valutazione d'impatto sulla protezione dei dati emerge che il trattamento è suscettibile di presentare un rischio elevato per l'interessato e non vengono intraprese misure per la mitigazione del rischio, è necessario rivolgersi alle autorità di controllo prima di procedere all'implementazione dei nuovi processi di trattamento dei dati.

8 SICUREZZA DEI DATI PERSONALI

I dati personali devono essere protetti contro possibili divulgazioni e accessi non autorizzati, nonché perdite, modifiche o distruzioni accidentali. Ciò vale indipendentemente da che il trattamento avvenga in formato elettronico o cartaceo.

I titolari e i responsabili del trattamento devono mettere in atto misure tecniche e organizzative adeguate per proteggere i dati da qualsiasi forma di abuso. Tali misure devono basarsi: (i) sulle best practice, (ii) sui rischi del trattamento e (iii) sulla necessità di protezione dei dati personali (determinata attraverso l'iter per la classificazione delle informazioni); esse includono, come di volta in volta opportuno:

(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.

Le misure tecniche e organizzative per la protezione dei dati personali sono parte del sistema interno di gestione della sicurezza informatica e devono essere costantemente adeguate in risposta agli sviluppi tecnici e ai cambiamenti organizzativi.

Le procedure di sicurezza devono includere come minimo:

- Controlli degli accessi: qualunque soggetto estraneo all'interno delle aree soggette a controllo degli accessi deve essere segnalato.

- Cassetti e armadi dotati di chiusure di sicurezza: la scrivania e gli armadi devono essere chiusi a chiave se contengono informazioni riservate di qualsiasi natura. I dati personali sono sempre informazioni riservate. I dipendenti devono assicurarsi che documenti e stampe contenenti dati personali non vengano lasciati in luoghi dove tutti possono vederli, ad esempio nella stampante. Se i dati vengono salvati su un supporto dati (ad esempio CD, chiavetta di memoria o DVD), il supporto deve essere conservato sotto chiave quando non viene utilizzato.
- Metodi di smaltimento: i documenti cartacei devono essere distrutti e smaltiti in sicurezza quando non sono più necessari; questo vale anche per i dati personali solitamente archiviati in formato elettronico, ma di cui sono state create stampe cartacee.

- Dati salvati su supporto elettronico: i dati personali devono essere protetti da password secondo la direttiva attuale sulle password e non devono essere condivise tra i dipendenti. Se ricevuti in formato elettronico, i dati personali devono poter essere salvati e aperti su sistemi server informatici e applicazioni IT strutturate, anziché in computer locali non crittografati.

- Dati personali acquisiti in formato elettronico messi a disposizione dall'interessato: occorre verificare l'identità dell'interessato, determinata preferibilmente mediante un doppio processo Opt-In (anche un secondo indirizzo e-mail per la convalida dell'indirizzo e-mail indicato). Se l'accesso a un sito web o a un'app è limitato agli utenti registrati (ad es. account utente), l'identificazione e l'autenticazione dell'interessato devono garantire una protezione di sicurezza proporzionata ai contenuti durante l'accesso.

- Cautela nella condivisione dei dati personali: i dati personali non dovrebbero essere condivisi in nessun caso; vale il principio di "informazione necessaria". È obbligatoria l'adozione di un concetto per la ripartizione e la separazione per singolo processo aziendale, nonché per l'implementazione di ruoli e competenze. I dati personali devono essere cifrati in vista della trasmissione in formato elettronico. Il responsabile IT può spiegare come inviare dati personali a persone di contatto esterne autorizzate.

- Richiesta di istruzioni: in caso di dubbi o incertezze su un qualsiasi aspetto della protezione dei dati o in merito agli obblighi previsti dalla presente Direttiva sulla privacy, è necessario avvalersi della consulenza di un diretto superiore, del garante della privacy eventualmente presente in loco o di Legal & Compliance.

Il GDPR esige che l'aspetto della privacy venga tenuto in considerazione il più precocemente possibile. Il rispetto della privacy fin dalla progettazione prevede che le organizzazioni considerino la questione della sfera privata già nelle primissime fasi della concezione tecnica e durante tutto il processo di sviluppo di nuovi prodotti, processi o servizi che hanno a che

fare con il trattamento dei dati. Con protezione della sfera privata per impostazione predefinita si intende che, se un sistema o un servizio include la decisione di un singolo su quanti dati personali dovrà condividere con gli altri, per quel sistema dovranno applicarsi le impostazioni predefinite in grado di assicurare la massima protezione per la sfera privata. Pertanto ogni nuova applicazione IT è soggetta a una procedura di autorizzazione finalizzata a verificarne nell'ambito delle normali valutazioni, anche l'idoneità dal punto di vista della protezione dei dati.

9 NOTIFICA DI INCIDENTI INERENTI LA SICUREZZA DEI DATI

Molte normative sulla privacy esigono una notifica diretta al legislatore degli incidenti inerenti la sicurezza dei dati. È pertanto obbligatorio segnalare tempestivamente tutti gli incidenti inerenti la sicurezza dei dati al coordinatore della protezione dei dati e/o al garante della privacy competente, indipendentemente dal fatto che sia coinvolto un sistema locale o di gruppo, applicando la procedura indicata nella direttiva di Arbonia sugli incidenti inerenti la sicurezza dei dati ("Arbonia Data Breach Policy"). Anche nel caso in cui l'IT rilevi possibili incidenti o rischi inerenti la sicurezza informatica, è obbligatorio darne comunicazione secondo la direttiva Data Breach Notification.

L'obiettivo è l'adempimento degli obblighi di segnalazione delle violazioni previsti dalle leggi applicabili in materia di protezione dei dati (ad es. ai sensi del GDPR al più tardi entro 72 ore dal rilevamento).

In tal caso l'accento deve essere posto sul rispetto dei termini per la notifica delle violazioni della privacy e devono essere immediatamente avviate le necessarie misure atte a indagare e stabilire se i dati personali sono stati effettivamente violati. Corporate IT deve tenere un registro interno delle violazioni della sicurezza in Arbonia, onde consentire il rispetto degli obblighi di notifica previsti dalle leggi nazionali applicabili e garantire l'applicazione delle regole di rappresentanza per assicurare la segnalazione puntuale e sistematica di qualsiasi violazione. Prima di effettuare una segnalazione a un'autorità nazionale, è necessario informare Corporate IT o la divisione Legal and Compliance di gruppo.

Devono essere rigorosamente rispettate tutte le direttive di Corporate IT e delle divisioni IT locali.

10 CONSEGUENZE DEL MANCATO RISPETTO

Il rispetto della presente Direttiva sulla privacy è di assoluta importanza per Arbonia e per l'immagine pubblica dell'azienda. In alcuni paesi il trattamento improprio dei dati personali può avere conseguenze penali gravi e giustificare eventuali richieste di risarcimento danni. Internamente ad Arbonia la violazione delle regole stabilite nella presente Direttiva sulla privacy possono comportare sanzioni previste per legge e/o in base al contratto (di lavoro) applicabile.

ARBONIA

11 DEROGHE

Eventuali deroghe rispetto alle disposizioni della presente direttiva e degli allegati sono consentite solo previa consultazione con l'Head of Legal & Compliance.

12 INFORMAZIONI

Informazioni relative alla presente Direttiva sulla privacy vengono fornite dall'Head of Legal & Compliance.

13 ENTRATA IN VIGORE

La presente direttiva entra in vigore il 17 giugno 2020 e sostituisce la direttiva relativa al trattamento dei dati (Informativa sulla privacy) del 5 dicembre 2013.

Arbon, 16 giugno 2020

Arbonia AG

Alexander von Witzleben
Presidente del consiglio d'amministrazione e CEO

Andrea Wickart
Head of Legal & Compliance / Segretaria generale

Documenti in aggiunta alla presente Direttiva sulla privacy:

I seguenti documenti aggiuntivi nelle rispettive versioni attuali concretizzano la presente Direttiva sulla privacy:

- Direttiva sulle richieste da parte degli interessati e sulla cancellazione dei dati
- Direttiva sulle violazioni dei dati personali
- Informativa per il trattamento dei dati personali dei dipendenti

Questo documento è valido senza firma.