Codice di condotta in materia di Protezione dei Dati Personali

C6.PLC.01

Versione 1.0

25 Aprile 2018

Note legali

Sommario

NOME	Codice di condotta in materia di Protezione dei Dati Personali
ID	C6.PLC.01
SUPERVISORE DEL PROCESSO	A.A. Ilyin, Chief Financial Officer, EuroChem Group
PROPRIETARIO DEL PROCESSO	V.V. Sidnev, General Counsel, EuroChem Group
SVILUPPATO DA	E.V. Kholmanskikh, Chief Compliance Officer, EuroChem Group
VERSIONE	1.0
DATA DI ENTRATA IN VIGORE	25 Aprile 2018
DATA DI APPROVAZIONE	24 Aprile 2018

Cronologia revisioni

Versione	Data di entrata in vigore	Scopo	Dettagli revisione
1.0	25 Aprile 2018		non applicabile

Indice

1. Termini e definizioni

A meno che non venga specificato diversamente, le parole ed espressioni che sono state definite (o espresse per essere soggette a un contesto particolare) nel Codice di Condotta e nel Codice di Condotta *Compliance* hanno lo stesso significato (o sono soggette allo stesso contesto) nel presente Codice di Condotta in materia di Protezione dei Dati Personali (in seguito denominato il "Codice").

Inoltre, si applicano le seguenti definizioni:

Termine	Definizione
"Dati personali"	indica qualsiasi informazione relativa ad una persona interessata identificata o identificabile; rappresenta una gamma molto ampia di dati identificativi personali, come ad esempio il nome di una persona fisica, numero telefonico (professionale), indirizzo elettronico (professionale), numero identificativo, dati relativi all'ubicazione, identificativo online, etc.
"Dati sensibili"	indica dati personali che rivelano l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, o appartenenze sindacali, e il trattamento dei dati genetici, di dati biometrici al fine di identificare in modo univoco una persona fisica, dati concernenti la salute o dati relativi alla vita sessuale o all'orientamento sessuale di una persona fisica.
"Titolare del Trattamento"	indica la persona fisica o giuridica, autorità pubblica, agenzia o altro ente che, singolarmente o congiuntamente ad altri, determina le finalità e i mezzi del trattamento di dati personali.
"Responsabile del trattamento"	indica una persona fisica o giuridica che elabora i dati personali per conto del Titolare del trattamento.
"Persona interessata"	indica ogni individuo che è l'interessato dei Dati personali detenuti dal Gruppo.
"Trattamento"	indica qualsiasi operazione o insieme di operazioni che è svolta/o su Dati Personali o su insiemi di dati personali, con o che senza mezzi automatizzati, quali la raccolta, registrazione, organizzazione, strutturazione, archiviazione, adattamento o alterazione, il reperimento, la divulgazione attraverso trasmissione, diffusione o altro metodo di messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione.
"Violazione dei Dati Personali"	indica una violazione della sicurezza che porta alla distruzione accidentale o illegale, alla perdita, alterazione, divulgazione non autorizzata di, o all'accesso a Dati personali trasmessi, archiviati o elaborati in qualsiasi altra forma.
"Consenso dell'interessato"	indica qualsiasi indicazione liberamente concessa, specifica,

	informata e inequivocabile della volontà dell'interessato in base alla quale acconsenta, mediante dichiarazione o azione chiaramente affermativa, al trattamento dei dati personali.
"Responsabile UE della Protezione dei Dati"	indica un dipendente del Gruppo che è responsabile dell'implementazione del Codice all'interno della parte UE del Gruppo
"Responsabile Globale della Protezione dei Dati"	indica un dipendente del Gruppo che è responsabile dell'implementazione del Codice all'interno del Gruppo
"Responsabile Locale della Protezione dei Dati"	indica un dipendente del Gruppo che è responsabile
"Contratto con un Responsabile del trattamento"	indica un accordo stipulato tra il Gruppo e qualsiasi controparte per l'implementazione del Codice all'interno del Gruppo pertinente.
"Piano di conservazione"	indica un piano speciale in base al quale i documenti sono conservati con tempistiche ben definite.

2. Applicazione

2.1. Uso previsto

Nel presente Codice vengono tracciati i principi chiave della Protezione dei Dati Personali e del Trattamento di Dati Personali, applicabili al Gruppo.

In qualità di datore di lavoro, cliente e fornitore, ciascun membro del Gruppo raccoglie e utilizza dati personali relativi ai dipendenti, partner commerciali, clienti, potenziali clienti, etc. Dato che la gestione di questi dati personali è indispensabile per le nostre operazioni, il Gruppo si rende conto che la protezione dei diritti personali e della *privacy* di ciascun individuo sia il fondamento della fiducia in tutte le relazioni. Per questo motivo, il Gruppo intende eccellere nella Protezione e nel corretto Trattamento dei Dati Personali.

Per il Gruppo è fondamentale rispettare i requisiti di Protezione dei Dati Personali nei paesi in cui viene svolta l'attività e dove risiede la persona interessata. Tutti i membri del Gruppo devono rispettare le normative locali di tutto il mondo che regolano il controllo e il trattamento dei dati personali.

La priorità principale del Gruppo è la garanzia di standard universalmente applicabili a livello mondiale per la gestione dei dati personali. Il presente Codice in materia di Protezione dei Dati Personali rappresenta il quadro generale applicabile a tutto il Gruppo. Date le variazioni delle normative locali e la diversità delle attività, è comunque inevitabile che l'implementazione di questi principi di Protezione Dati possa variare leggermente per i vari membri del Gruppo.

Il presente Codice deve essere portata a conoscenza di tutti i dipendenti che devono rispettare lo stesso Codice e adempiere ai suoi requisiti. Inoltre, il Codice si applica alle controparti che hanno un rapporto con un membro del Gruppo e che hanno o potrebbero avere accesso a Dati personali. Queste controparti dovranno leggere, comprendere e rispettare il presente Codice.

2.2. Area di applicazione e requisiti legali obbligatori

I paesi in cui il Gruppo conduce gli affari, possono essere divisi in tre grandi gruppi a seconda dell'ubicazione: UE, Russia e altri paesi.

Ad eccezione delle sedi centrali in Svizzera e Russia, alcuni membri del Gruppo si trovano nell'UE. Le norme dell'UE sulla Protezione dei Dati (Regolamento (UE) 2016/679 (d'ora in avanti indicato come "GDPR" o Regolamento Generale sulla Protezione dei Dati) sono vincolanti e si applicano su base armonizzata in tutto il territorio dell'UE. Il campo di applicazione del GDPR è più ampio dell'area UE, poiché si estende anche ai membri del Gruppo con sede al di fuori dell'UE se la persona interessata è residente nell'UE.

Il Gruppo si è assunto l'impegno di utilizzare i principi e gli obblighi previsti dal GPDR come modello per il proprio Codice di Condotta in materia di Protezione dei Dati Personali. Tuttavia, i singoli membri del Gruppo devono anche rispettare le normative locali. Il presente Codice in

materia di Protezione dei Dati Personali è da considerarsi un'integrazione alle normative locali in materia di Protezione dei Dati. Il regolamento locale pertinente ha la precedenza nel caso in cui vi sia conflitto con il presente Codice in materia di Protezione dei Dati personali o abbia requisiti più severi rispetto al presente Codice in materia di Protezione dei Dati Personali. Esempi di regolamenti locali che sono rilevanti per alcuni membri del Gruppo includono:

- Legge Federale № 152-FZ sui dati personali del 2006 (applicabile per la Russia);
- Legge Federale sulla Protezione dei Dati (FADP) del 19 giugno 1992 (applicabile per la Svizzera);
- Legislazione locale in materia di *corporate governance* di tempi di conservazione dei dati.

3. Disposizioni generali

3.1. Obiettivi del Codice

I principali obiettivi del Codice sono i seguenti:

- Proteggere le libertà e i diritti di tutte le persone interessate e informarle sugli stessi;
- Trattare dati personali in modo corretto;
- Evitare qualsiasi violazione dei dati personali e problemi di sicurezza in generale;
- Incrementare la consapevolezza del regime di Protezione dei Dati Personali in generale.

3.2. Principi del Codice

Ogni trattamento di Dati Personali dovrà essere condotto in conformità con i principi di Protezione dei Dati personali come stabilito nel GDPR. I codici di condotta e le procedure del Gruppo sono progettate per garantire il rispetto di questi principi.

In breve, noi, come Gruppo, ci impegniamo a rispettare i seguenti principi:

- Il principio di lealtà e legalità: ci impegniamo a trattare i dati personali esclusivamente nella misura in cui abbiamo informato la persona interessata e nella misura in cui esiste una base legale per il trattamento.

- Il principio di limitazione delle finalità: tratteremo i dati personali esclusivamente per scopi specifici, espliciti e legittimi e non tratteremo ulteriormente questi dati in un modo che non sia compatibile con tali scopi.

- Il principio di minimizzazione dei dati: tratteremo esclusivamente i dati personali che siano adeguati, pertinenti e limitati a quanto necessario in relazione agli scopi per i quali questi dati vengono trattati.

- Il principio di accuratezza: tratteremo esclusivamente dati che siano accurati e, ove necessario, aggiornati. Adotteremo tutte le misure ragionevoli al fine di garantire che i dati personali inadeguati vengano senza indugio cancellati o rettificati.

- Il principio di limitazione del trattamento: terremo tutti i dati personali in una forma che consenta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per gli scopi per i quali i dati personali vengono trattati.

- Il principio di sicurezza: tratteremo esclusivamente i dati in modo tale da garantire una sicurezza appropriata, inclusa la protezione da trattamenti non autorizzati o illegali, da perdite accidentali, distruzione o danni, utilizzando tutte le misure tecniche o organizzative appropriate.

- Il principio di responsabilità: il rispetto dei suddetti principi di Protezione dei Dati sia verso le autorità competenti che verso le persone interessate è nostra responsabilità e saremo in qualsiasi momento in grado di dimostrarlo.

4. Misure per la Protezione dei Dati

L'impegno del Gruppo nell'attuazione dei suddetti principi di Protezione dei Dati è illustrato dalle seguenti misure adottate:

4.1. Trattamento leale e lecito

Il Gruppo assicura che i dati sono raccolti e trattati in modo leale e lecito. Adottiamo tutte le misure ragionevoli per garantire che i dati personali siano aggiornati, accurati e conservati per un periodo di tempo predefinito.

Il Gruppo assicura che, a seconda della categoria a cui appartiene la persona interessata, i dati raccolti saranno utilizzati esclusivamente sulle basi leali e legittime descritte in seguito.

4.1.1. Dati dei dipendenti

"Dati dei dipendenti" indica tutti i dati trattati da qualsiasi membro del Gruppo relativi ai dipendenti e (se richiesto) ai loro coniugi. Tuttavia, i dati dei dipendenti sono più ampi dei semplici dati personali dei dipendenti attuali. Esistono anche altre categorie di dati relativi all'occupazione, come i dati sui dipendenti pensionati e i potenziali candidati.

Tutti i dati dei dipendenti sono raccolti dal Gruppo nel quale è impiegato il dipendente. Il datore di lavoro è considerato il Titolare del trattamento dei dati (ciò significa che il Gruppo determina le finalità e gli strumenti del trattamento dei dati).

1. Fondamento giuridico per le attività di trattamento

Nel rapporto di lavoro, la stragrande maggioranza delle attività di trattamento dei dati è legittimata dalla necessità dell'esecuzione di un contratto: i membri del Gruppo non sarebbero in grado di eseguire correttamente i propri obblighi relativi ai contratti di lavoro, senza essere in grado di trattare i dati dei propri dipendenti.

Alcune attività di trattamento dei dati sono legittimate da un obbligo legale: in tutti i paesi in cui i membri del Gruppo svolgono attività commerciali, vi è l'obbligo legale di trattare alcuni dati personali dei dipendenti, ad es. per motivi di sicurezza sociale, assicurazioni, pagamento degli stipendi, etc.

Alcune delle attività di trattamento dei dati potrebbero anche essere consentite in base a un accordo collettivo. I contratti collettivi sono accordi su fasce salariali o accordi tra datori di lavoro e rappresentanti dei lavoratori, nell'ambito di applicazione previsto dalla legge sul lavoro. L'accordo deve coprire la finalità specifica dell'attività di trattamento dei dati prevista, e deve essere redatto nell'ambito dei parametri della legislazione nazionale sulla Protezione dei Dati.

Ciascun membro del Gruppo può, in quasi tutti i casi, fare affidamento su interessi legittimi per il trattamento dei dati personali, poiché lo stesso è necessario per il corretto funzionamento della propria attività (ad esempio, mentre un membro del Gruppo non ha stipulato un contratto di lavoro con i candidati, ma il Gruppo ha un legittimo interesse a valutare potenziali candidati, soprattutto quando avviano il processo di richiesta contattando il membro del Gruppo).

In un numero molto limitato di casi, l'attività di trattamento dati potrebbe dover essere legittimata dal consenso esplicito dato dal dipendente (ad es. pubblicando un'intervista o una fotografia in una rivista interna, etc.)

Ogni membro del Gruppo è l'unico responsabile dell'identificazione delle basi giuridiche dell'attività di trattamento.

2. Trattamento leale

Una panoramica dettagliata sulle modalità di trattamento dei dati dei dipendenti può essere trovata nei nostri codici di condotta più dettagliati. In questa sede forniamo soltanto una breve presentazione di alcuni aspetti dell'attività di trattamento:

- Minimizzazione: il Gruppo garantisce che tutti i dati dei dipendenti che vengono trattati siano limitati al minimo.
- Accuratezza: il Gruppo garantisce che tutti i dati dei dipendenti siano regolarmente aggiornati a livello dell'intera organizzazione e che ciascun dipendente possa in qualsiasi momento chiedere la correzione di eventuali dati errati.
- Limite di archiviazione: tutti i dati dei dipendenti saranno trattati nel corso della durata del contratto di lavoro. Al termine del contratto di lavoro, gran parte dei dati saranno cancellati una volta che il periodo di conservazione richiesto è stato rispettato, salvo diversamente richiesto dalla legge o nel caso in cui la persona interessata abbia

esplicitamente acconsentito a rimanere in archivio per ulteriori attività specifiche di trattamento.

- Sicurezza: tutti i dati personali vengono trattati in modo sicuro. Ad es. l'accesso ai dati è limitato in base alla necessità di sapere, il Gruppo spesso trasferisce i dati sotto pseudonimo a terzi, etc.
- Trattamento dei dati sensibili: i dati sensibili, quali razza e origini etniche, opinioni politiche, religiose o filosofiche, appartenenza ai sindacati, e i dati relativi alla salute e alla vita sessuale dell' interessato saranno trattati con la dovuta maggiore attenzione.
- Il Gruppo riduce al minimo il trattamento automatico di dati personali. Se i dati personali sono trattati in modo automatico come parte del rapporto di lavoro e vengono valutati specifici personali dei dati (es. nell'ambito della selezione del personale o della valutazione di profili di competenze), tale trattamento automatico non potrà essere l'unica base per decisioni che potrebbero avere conseguenze negative o comportare problemi significativi per il dipendente interessato.

Ogni membro del Gruppo è l'unico responsabile del trattamento leale dei dati dei dipendenti.

4.1.2. Dati delle Controparti

"Dati delle Controparti" indica i dati personali di clienti, subappaltatori, fornitori, partner commerciali, utenti del sito, etc. Mentre questi saranno sempre considerati dati professionali, nel senso che tendenzialmente non saranno trattati dei dati sensibili, ciascun indirizzo e-mail o numero telefonico sarà considerato come dato personale.

Nella misura in cui il Gruppo ha raccolto i dati delle Controparti direttamente dall'interessato, esso fungerà da Titolare del trattamento. La natura dell'attività commerciale del Gruppo potrebbe necessitare che i dati delle Controparti siano raccolte da un'altra Parte. In questo caso, il Gruppo sarà solo Responsabile del Trattamento e non Titolare del Trattamento, salvo diversamente concordato.

1. Fondamento giuridico per le attività di trattamento dati

Nel rapporto contrattuale, la maggior parte delle attività di trattamento dei dati è legittimata dalla necessità di esecuzione di un contratto: il Gruppo non sarebbe in grado di svolgere in modo appropriato i propri obblighi ai sensi dei contratti, senza poter trattare i dati pertinenti.

Alcune attività di trattamento dati sono legittimate da un obbligo legale: in alcuni paesi dove il Gruppo svolge la sua attività commerciale, sussiste un obbligo legale di trattare alcuni dati personali dei fornitori.

Il Gruppo può, in quasi tutti i casi, fare affidamento su interessi legittimi per il trattamento dei dati personali, poiché è necessario per il corretto funzionamento della sua attività commerciale.

In un numero molto limitato di casi, l'attività di trattamento dati potrebbero dover essere legittimata dall'esplicito consenso dato da terzi (es. ricezione di una newsletter del Gruppo, etc.).

Nella misura in cui i Dati delle Controparti sono controllati dal Gruppo (nel senso che un membro del Gruppo determina le finalità e gli strumenti del trattamento dei dati), questo Gruppo sarà responsabile dell'identificazione dei fondamenti giuridici dell'attività di trattamento.

2. Trattamento leale

Una panoramica dettagliata sulle modalità di trattamento dei dati delle Controparti, può essere trovata nei nostri Codici di condotta più dettagliati. In termini generali, si applicano gli stessi principi di quelli applicabili al trattamento dei dati dei dipendenti come descritto in 4.1.1.

I seguenti principi aggiuntivi sono degni di nota:

- Nel caso in cui il trattamento dei dati delle Controparti sia raccolto attraverso il sito web del Gruppo e strumenti online: se i dati personali sono raccolti, trattati e utilizzati su siti web, le persone interessate ne saranno informati in un'informativa sulla *Privacy* e, se applicabile nell'informativa sui *cookies*. L'informativa sulla *Privacy* e qualsiasi informativa sui *cookies* saranno integrate cosicché siano facili da identificare, direttamente accessibili e costantemente disponibili per gli interessati.
  Nella misura in cui creiamo profili utenti (tracciatura) sui nostri siti web, le persone interessate saranno sempre informate secondo i criteri dell'informativa sulla *Privacy.* La tracciatura personale può essere effettuata esclusivamente se consentita dalle leggi nazionali o dietro consenso dell'interessato.

  Se siti web o app possono accedere ai dati personali in un'area riservata agli utenti registrati, l'identificazione e autenticazione della persona interessata offrirà una protezione sufficiente durante l'accesso.

- Marketing digitale: il Gruppo dovrà condurre le strategie di marketing digitale in un contesto principalmente *business to business,* dove non vi è alcun obbligo giuridico di ottenere il consenso per effettuare marketing digitale a soggetti a condizione che essi abbiano la possibilità di *opt-out.*

  Tuttavia, come regola generale, il Gruppo si impegnerà al fine di ottenere sempre il consenso prima di inviare materiale promozionale o di *direct marketing* alla persona interessata di una Controparte.

Nella misura in cui il Gruppo è il Titolare del trattamento dei dati delle Controparti, il Gruppo sarà responsabile nell'identificazione dei fondamenti giuridici dell'attività di trattamento.

4.1.3. Consenso

Nella misura in cui il Gruppo si affida al consenso come fondamento giuridico per il trattamento dei dati, si applicheranno le seguenti condizioni:

Dichiarazioni di consenso saranno spontaneamente trasmesse, per iscritto e in conformità con i regolamenti locali. Qualsiasi consenso che non soddisfi queste condizioni, è nullo. La dichiarazione di consenso sarà ottenuta per iscritto o elettronicamente ai fini della documentazione. Prima di

rilasciare il consenso, la persona interessata sarà informata riguardo alla portata delle attività di trattamento. Gli interessati possono revocare il consenso in qualunque momento.

Per i Dati sensibili, si deve ottenere il consenso esplicito scritto salvo nel caso in cui esista un chiaro fondamento giuridico alternativo per il trattamento dei dati.

Nella maggior parte dei casi, il consenso all'elaborazione dei Dati Personali e Sensibili è ottenuto sistematicamente dal Gruppo utilizzando documenti di consenso standard.

4.2. Protezione dei diritti delle persone interessate

Ciascun membro del Gruppo garantisce che la persona interessata i cui Dati Personali vengono trattati dal Gruppo potrà esercitare i seguenti diritti individuali.

- **Diritto ad essere informato:**

  Il Codice fornisce una panoramica completa dei principi generali in base ai quali il Gruppo tratta i Dati personali. Lo stesso è condiviso con gli interessati al momento della raccolta dei loro Dati Personali (nella misura in cui il Gruppo è il Titolare del trattamento) ed è disponibile pubblicamente su www.eurochemgroup.ru.

  Tuttavia, nel caso in cui la persona interessata lo richieda esplicitamente, il membro pertinente del Gruppo (intendendo il Titolare del trattamento o Responsabile del trattamento dei Dati personali) fornirà all'interessato le informazioni relative ai suoi Dati personali in modo conciso, trasparente, comprensibile e facilmente accessibile. Il Gruppo si riserva il diritto di rifiutare una richiesta di informazioni fintanto che la persona interessata abbia già ottenuto le informazioni o se ciò comportasse uno sforzo eccessivo per fornirle.

  Su richiesta, il Gruppo dovrà fornire le seguenti informazioni: 1) nome e dettagli di contatto dell'organizzazione, 2) le finalità del trattamento 3) i fondamenti giuridici per il trattamento; 4) le categorie di Dati personali ottenute; 5) i destinatari o le categorie di destinatari dei dati personali, 6) i dettagli relativi ai trasferimenti dei Dati personali a paesi terzi o organizzazioni internazionali (se applicabile), 7) i periodi di conservazione dei dati personali, 8) i diritti disponibili agli interessati concernente il trattamento, 9) il diritto a revocare il consenso (se applicabile), 10) il diritto di presentare un reclamo all'autorità di sorveglianza.

- **Diritto di accesso ai propri dati:**

  Al fine di garantire che gli interessati siano consapevoli di e possano verificare la legittimità delle attività di trattamento dati, il Gruppo garantisce loro il diritto di ottenere conferma che i dati della persona interessata vengono trattati; l'accesso ai dati personali; e altre

informazioni supplementari necessarie. Il formato dell'accesso deve essere stabilito di comune accordo.

- Diritto di rettifica:

  Nel caso in cui un membro del Gruppo tratti dei dati personali inaccurati o incompleti, la persona interessata può chiederne la rettifica o il completamento. Pertanto, il Gruppo si riserva il diritto di rifiutare una richiesta di rettifica se consentito da una normativa applicabile.

- Diritto di cancellazione e diritto di limitazione del trattamento:

  La persona interessata ha il diritto ad ottenere la cancellazione dei propri Dati personali dagli archivi del Gruppo, se 1) i Dati personali non sono più necessari per lo scopo originale della raccolta o del trattamento; 2) un membro del Gruppo si basa esclusivamente sul consenso come fondamento giuridico per il possesso dei dati, e l'interessato ritira il proprio consenso; 3) un membro del Gruppo si basa esclusivamente sugli interessi legittimi come base per il trattamento, l'interessato si oppone al trattamento dei dati e non vi è alcun interesse legittimo prioritario a continuare questo trattamento; 4) un membro del Gruppo elabora i Dati personali per scopi di *direct marketing*; 5) un membro del Gruppo ha trattato i dati personali in modo illegittimo.

  In alternativa alla richiesta di cancellazione dei dati personali, l'interessato può richiedere ad un membro pertinente del Gruppo di limitare il trattamento dei propri Dati Personali alla loro archiviazione, ma senza utilizzarli in altro modo. Tale limitazione può essere richiesta se: 1) l'interessato contesta l'esattezza dei propri Dati Personali; 2) i dati sono stati trattati in modo illegittimo e l'interessato oppone invece cancellazione e limitazione; 3) un membro del Gruppo non necessita ulteriormente dei Dati Personali ma la persona interessata necessita che i Dati Personali vengano conservati al fine di stabilire, esercitare o difendere un diritto; 4) l'interessato ha sollevato obiezioni contro un membro del Gruppo che tratta i dati e il membro sta intanto valutando se i suoi motivi legittimi prevalgono su quelli dell'interessato.

- Diritto di portabilità dei dati:

  In condizioni rigorose, la persona interessata può richiedere a un membro del Gruppo di fornirgli tutti i Dati Personali in forma strutturata, comunemente usata e leggibile da una macchina. Ciò dovrebbe consentire all'interessato di trasmettere i propri dati ad un'altra organizzazione. Se ciò è tecnicamente fattibile, l'interessato può richiedere di trasmettere i dati direttamente a questa altra organizzazione.

Il diritto alla portabilità dei dati si applica esclusivamente: 1) ai Dati Personali forniti da una persona fisica ad un Titolare del trattamento; 2) nei casi in cui il trattamento è basato sul consenso dell'interessato o per l'esecuzione di un contratto; e 3) quando il trattamento è svolto con strumenti automatici.

- **Diritto di sollevare obiezioni:**

  Se una persona interessata solleva un obiezione contro il trattamento dei propri Dati Personali per "motivi pertinenti alla propria situazione particolare", l'interessato ha il diritto di fare obiezione a: 1) trattamento basato su legittimi interessi e 2) *direct marketing* (inclusa la profilazione).

  In questo caso, un membro del Gruppo porrà termine al trattamento the Dati Personali a meno che: 1) possa dimostrare i validi motivi legittimi per il trattamento, che prevalgono sugli interessi, diritti e libertà dell'interessato; o 2) il trattamento è per l'istituzione, l'esercizio o la difesa di contestazioni legali.

Tutte le richieste per l'esercizio dei succitati diritti, devono essere indirizzate al Responsabile della Protezione dei Dati. Salvo diversamente consentito in base a regolamenti applicabili, ciascuna richiesta deve essere fatta per iscritto.

Salvo diversamente disposto da un regolamento applicabile, una risposta a ciascuna richiesta sarà fornita entro 30 giorni dalla ricezione della richiesta scritta da parte della persona interessata. Una verifica appropriata dovrà confermare che il richiedente è l'interessato o il legale rappresentante dello stesso.

Salvo diversamente disposto da un regolamento applicabile, ciascuna richiesta sarà gratuita a meno che la richiesta non sia ritenuta inutile o di natura eccessiva.

4.3. Sicurezza dei Dati Personali

Il Gruppo si impegna a conformarsi a quelle che vengono considerate le migliori prassi nel settore della sicurezza informatico.

Oltre a ciò, ciascuna Società del Gruppo ha adottato misure fisiche, tecniche e organizzative per garantire la sicurezza dei dati personali. Ciò include la prevenzione di perdite o danni, modifiche non autorizzate, accesso o trattamento, e altri rischi ai quali possono essere esposti in virtù dell'azione umana o dell'ambiente materiale o naturale.

Mentre le misure di sicurezza variano e dipendono dai membri del Gruppo, le misure seguenti sono considerate garanzie minime:

Tutti i Dati Personali sono trattati con la massima sicurezza e devono essere conservati:

- in un locale chiudibile a chiave con accesso controllato; e/o
- in un cassetto o archivio chiudibile a chiave; e/o
- se in formato elettronico, protetti da password in linea con i requisiti aziendali; e/o
- archiviati su supporti informatici (portatili) cifrati.

I registri manuali non devono essere lasciati in luoghi accessibili a personale non autorizzato e non possono essere allontanati dai locali commerciali senza autorizzazione speciale. Non appena i registri manuali non sono più necessari per l'assistenza giornaliera dei clienti, gli stessi devono essere rimossi dal sistema di archiviazione protetto.

I Dati personali possono essere cancellati o smaltiti esclusivamente in linea con il Piano di conservazione.

Il Gruppo deve assicurare che i Dati Personali non vengano divulgati a controparti non autorizzate inclusi i membri della famiglia, amici, organi governativi salvo nei casi richiesti dalla legge. Tutte le richieste di fornitura dei dati per una di queste ragioni devono essere supportate da documentazione opportuna e tali divulgazioni devono essere specificatamente autorizzate dal Responsabile della Protezione dei Dati.

Ogni membro del Gruppo garantisce che tutti i dipendenti aderiscano al presente Codice e ai Codici di Condotta. Inoltre, ogni membro del Gruppo garantisce che tutti i dipendenti che sono responsabili per l'esecuzione del Codice siano formati, informati e supportati in modo appropriato (vedi anche paragrafo 4.6)

4.4. Violazione dei Dati Personali

Una Violazione dei Dati Personali è una violazione della sicurezza che porta alla distruzione accidentale o illegittima, alla perdita, modifica, divulgazione non autorizzata di, o all'accesso a Dati Personali trasmessi, archiviati o trattati diversamente. Ciò potrebbe verificarsi a causa di un evento materiale o tecnico. Dato che tali violazioni avvengono sempre all'improvviso, ogni membro del Gruppo ha adottato tutte le precauzioni ragionevoli per evitare che una violazione dei dati personali si trasformi in una catastrofe.

Ogni membro del Gruppo ha implementato valide procedure di rilevazione, investigazione e comunicazione di violazioni. Esse sono descritte nel Codice di Condotta in materia di violazione dei dati delle Società del Gruppo. Inoltre, ciascun membro del Gruppo conserva un registro delle violazioni dei dati nei quali registra le informazioni relative ai fatti legati alla violazione dei dati personali, gli effetti delle violazioni e il dispendio e le azioni correttive adottati.

Mentre i codici di condotta dei vari membri potrebbero variare, ciascuna procedura di violazione dei dati conterrà i seguenti passaggi:

- Tutti i dipendenti devono informare immediatamente il loro supervisore riguardo i casi di violazione contro il presente Codice in materia di Protezione dei Dati Personali (Incidenti relativi alla Protezione dei Dati). Il supervisore informerà quindi il Responsabile Locale della Protezione dei Dati, il Responsabile UE della Protezione dei Dati e il Responsabile Globale della Protezione dei Dati.

- I Responsabili della Protezione dei Dati decidono se l'incidente relativo alla Protezione Dati risulta da una violazione di dati personali. Per esempio, chiavette USB smarrite, computer portatili rubati, infezioni di programmi malware o database hackerati che contengono dati personali, sono tutte considerate violazioni di dati personali. Una minaccia o un difetto nelle misure di sicurezza, come password deboli o firewall obsoleti non sono considerati una violazione dei dati personali fintanto che non sono trapelati dati personali.

- Se l'incidente relativo alla Protezione dei Dati rappresenta invece una violazione dei dati personali, i Responsabili della Protezione dei Dati investigheranno sulla portata della violazione. Esamineranno la portata della violazione dei dati personali, quanti interessati potrebbero riguardare, se la violazione potrebbe risultare in un rischio alla libertà e ai diritti degli interessati, se i dati personali compromessi contengono Dati Sensibili, se i dati compromessi erano protetti (criptati o altro), se altre parti potrebbero essere coinvolte nella violazione dei dati e quali misure potrebbero essere intraprese per mitigare le (ulteriori) perdite di Dati Personali.

- In base alla suddetta valutazione, i Responsabili della Protezione dei Dati decideranno se l'Autorità di Vigilanza e la persona interessata devono essere informati della violazione. La notifica all'Autorità di Vigilanza non è necessaria se è improbabile che la violazione dei Dati Personali risulti in un rischio per i diritti e le libertà dei soggetti.

- Se è necessaria una notifica della violazione dei dati personali, allora il Gruppo informerà l'Autorità di Vigilanza competente e fornirà loro tutte le informazioni necessarie entro 72 ore dopo esserne venuto a conoscenza.

- Laddove la violazione dei dati personali possa probabilmente risultare in un "rischio elevato" per i diritti e le libertà delle persone, il Gruppo informerà direttamente gli interessati. Un "rischio elevato" indica che la soglia per la notifica ai soggetti è più alta di quella necessaria alla notifica presso l'Autorità di Vigilanza pertinente. Se le notifiche individuali fossero uno sforzo sproporzionato, il Gruppo può utilizzare una qualsiasi forma di comunicazione pubblica che sia egualmente efficace nell'informare gli interessati.

- Al fine di mantenere l'alto livello di visibilità e trasparenza, ogni membro del Gruppo documenterà tutti gli incidenti relativi alla Protezione dei Dati (sia segnalati che non), inclusi i fatti legati alla violazione, i suoi effetti e le azioni intraprese o pianificate. Tutta

questa documentazione permetterà all'Autorità di Vigilanza di verificare la conformità con gli obblighi di notifica. Tutti i fatti relativa alla violazione dei dati devono essere registrati in uno strumento specifico "Registro delle Violazioni di Dati" (Allegato 2).

4.5. Conservazione e smaltimento dei dati

Come già trattato nel paragrafo 4.1 del presente Codice, i Dati personali non possono essere trattati per un periodo più lungo di quello necessario alle finalità del loro trattamento.

Ogni membro ha definito e implementato un Piano di conservazione separato conformemente all'Allegato 3. I periodi di conservazione sono basati sui requisiti delle legislazioni locali per differenti tipi di categorie di Dati Personali. Solitamente la legislazione locale classifica i dati personali come di seguito:

1. Contabili e finanziari
2. Contratti
3. Registrazioni aziendali
4. Corrispondenza e Memorandum interni
5. E-mail e altre comunicazioni di tipo elettronico
6. Pratiche e documenti legali
7. Buste paghe
8. Documenti pensionistici
9. Registrazioni personali
10. Registrazioni fiscali

In ogni caso, tutti i dati personali saranno trattenuti per un periodo minimo che permetta al Gruppo di presentare un'istanza o di difendersi in tribunale in base alle legislazioni locali.

4.6. Formazione del personale

Il Gruppo garantisce che a tutti i dipendenti che abbiano accesso ai Dati personali saranno illustrate tutte le responsabilità relative al presente Codice come parte della formazione iniziale del personale. Inoltre, ciascun membro del Gruppo fornirà una formazione continua relativa alla Protezione dei Dati e dell'orientamento sulle procedure ai loro dipendenti.

Il Responsabile Locale della Protezione dei Dati è responsabile dell'implementazione di corsi di formazione adeguati per tutti i Dipendenti. La forma di tali corsi può variare in base al gruppo target, al numero di dipendenti che devono essere formati, agli obiettivi della formazione e ad altre circostanze.

La formazione deve essere effettuata con regolarità. Ogni membro del Gruppo stabilisce autonomamente la tempistica effettiva che deve essere conforme ai requisiti/alle proposte del Responsabile UE o Globale della Protezione dei Dati.

4.7. Registrazioni delle attività di trattamento

Ogni Società del Gruppo ha identificato tutti i Dati Personali che tratta e controlla e li conserva in un Registro dei Dati (Allegato 4).

Questo Registro dei Dati garantisce che le Società del Gruppo rispettano alcuni dei principali requisiti di responsabilità richiesti dal GDPR:

- Tenuta di registrazioni su tutte le attività di trattamento dati;
- Tenuta di registrazioni sugli accordi del Responsabile del Trattamento;
- Tenuta di registrazioni sulle violazioni dei dati, incluse le notifiche di violazione alle autorità di vigilanza e alle persone interessate.

Mentre il contenuto del Registro dei Dati potrebbe variare tra membri del Gruppo, esso contiene almeno i dati seguenti relativi alle attività di trattamento dati:

- il nome e i dettagli di contatto del Gruppo e, dove applicabile, il (co-) Titolare del trattamento e il suo rappresentante;
- le finalità delle attività di trattamento dati;
- una descrizione delle categorie delle persone interessate e delle categorie di dati personali;
- le categorie di destinatari ai quali i Dati Personali sono stati o saranno divulgati, inclusi i destinatari di paesi terzi o organizzazioni internazionali;
- ove applicabile, i trasferimenti di Dati Personali a paesi terzi o a organizzazioni internazionali, inclusa l'identificazione di tale paese terzo o organizzazione internazionale;
- ove possibile, i termini previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate dal Gruppo.

Ogni membro del Gruppo è l'unico responsabile unicamente per la tenuta del registro.

4.8. Trasferimento dati

Al fine di controbilanciare una possibile mancanza nella Protezione dei Dati, i trasferimenti dei Dati personali a controparti, è soggetta a misure di sicurezza aggiuntive. Il Gruppo ha identificato tre diverse tipologie di trasferimenti di dati all'interno della sua organizzazione, con differenti insiemi di misure di sicurezza:

- Trasferimenti di dati all'interno del Gruppo: allo scopo di facilitare il trasferimento di dati saranno implementate Norme Aziendali Vincolanti. Queste norme sono approvate dall'Autorità di Vigilanza e sono giuridicamente vincolanti per tutti i membri del Gruppo. Tra l'altro, queste Norme Aziendali Vincolanti specificano le finalità del trasferimento e le categorie di dati in questione; riflettono i requisiti del GDPR; confermano che gli esportatori di dati con sede nell'UE accettano la responsabilità per conto dell'intero Gruppo; spiegano le procedure di reclamo e forniscono i meccanismi che garantiscono la conformità (es. audit).

- Trasferimenti di Dati alle controparti all'interno dello Spazio Economico Europeo (o uno degli altri paesi considerati come garanti della stessa protezione) che agiscono come Responsabile del trattamento: questi trasferimenti di dati avvengono in conformità al GDPR.

  Prima di trasferire qualsiasi dato a terzi, ciascun membro del Gruppo ha effettuato indagini attraverso processi di *due diligence* e ha valutato se questa controparte agisce in conformità alle normative applicabili.

  A seguito di questa valutazione, ogni membro del Gruppo deve concludere un accordo con ciascuna di questi Responsabili esterni del trattamento (Contratto con Responsabile esterno del trattamento). Tutti questi accordi contengono almeno le seguenti informazioni:

- per i trasferimenti di dati a entità esterne al Gruppo al di fuori dello Spazio Economico Europeo e per quanto sia applicabile il GDPR (da intendersi: un membro del Gruppo ha sede all'interno dell'UE o la persona interessata risiede nell' UE):

  Oltre alla stipula del succitato Contratto con il Responsabile del trattamento dati, ciascun membro del Gruppo deve controllare se la controparte alla quale i Dati personali saranno inviati mantenga adeguate misure di sicurezza aggiuntive. Se tale misure di sicurezza non sono state adottate, allora il Gruppo non trasferisce alcuna informazione a questa terza parte.

4.9. Valutazione d'impatto sulla Protezione dei Dati

Per assicurare che tutti i requisiti della Protezione dei Dati siano automaticamente identificati e indirizzati nella progettazione di nuovi sistemi o processi e/o durante la revisione o espansione di sistemi o processi esistenti, ciascun membro del Gruppo deve garantire che la Valutazione d'impatto sulla Protezione dei Dati (DPIA) sia effettuata per tutti i sistemi o processi nuovi e/o esistenti che sono sotto la sua responsabilità.

Questo DPIA è effettuato in collaborazione con il Responsabile UE della Protezione dei Dati e con il Responsabile Globale. Dove applicabile, il reparto IT, come parte del proprio sistema informatico e del processo di revisione del design delle applicazioni, coopererà con il Responsabile della Protezione dei Dati per la valutazione dell'impatto di qualsiasi nuova tecnologia utilizzata sulla sicurezza dei dati personali.

4.10. Responsabili della Protezione dei Dati

4.10.1. I Responsabili della Protezione dei Dati

Poiché il Gruppo opera in diverse giurisdizioni, inclusa l'UE, vengono nominati più Responsabili della Protezione dei Dati:

- Il Responsabile Globale della Protezione dei Dati (responsabile per il Gruppo):

  Il Responsabile Globale della Protezione dei Dati è nominato e rimosso dalla sua posizione dal CEO, previa consultazione con il General Counsel e il CFO.

  Il Responsabile Globale della Protezione dei Dati del Gruppo è Aleksander Pusanov. I suoi dettagli di contatto sono: Aleksander.Puzanov@eurochem.ru.

  Il Responsabile UE della Protezione dei Dati (responsabile per le attività UE del Gruppo):

  Il Responsabile UE della Protezione dei Dati è nominato e rimosso dalla sua posizione dal CEO, previa consultazione con il Responsabile Globale della Protezione dei Dati.

  Il Responsabile UE della Protezione dei Dati del Gruppo è Pieter Callens. I suoi dettagli di contatto sono: Pieter.Callens@eurochem.be

  I Responsabili locali della Protezione dei Dati (responsabili per un membro del Gruppo, se designato):

Ciascun membro del Gruppo può nominare un Responsabile Locale della Protezione dei Dati. Il Responsabile Locale della Protezione dei Dati è nominato e rimosso dalla sua posizione dal CEO/direttore generale del membro del Gruppo. Nel caso in cui non sia stato nominato nessun Responsabile Locale della Protezione dei Dati, il CEO/direttore generale fungerà da Responsabile Locale della Protezione dei Dati.

4.10.2. Doveri dei Responsabili della Protezione dei Dati

Responsabile Globale della Protezione dei Dati

Il Responsabile Globale della Protezione dei Dati dovrà essere nominato sulla base di qualità professionali e, in particolare, per la conoscenza approfondita della legislazione e delle pratiche in materia di Protezione dei Dati e alla capacità di adempiere ai seguenti doveri in qualità di Responsabile Globale della Protezione dei Dati:

- fornire consulenza al management del Gruppo sugli argomenti relativi al Codice e per supportarlo in relazione ai principali rischi, preoccupazioni e questioni in materia di Protezione dei Dati non appena si verifichino;
- stabilire e garantire un Sistema di Protezione dei Dati di alta qualità all'interno del Gruppo;
- gestire le comunicazioni, strategie e iniziative educative o formative e garantire sostegno alle *Business Unit* negli ambiti di Protezione dei Dati come richiesto;
- vigilare sul Responsabile UE della Protezione dei Dati e sui Responsabili Locali della Protezione dei Dati (se nominati) .

In collaborazione con il Responsabile UE della Protezione dei Dati e i Responsabili Locali della Protezione dei Dati (se nominati):

- assicurare che procedure e codici di condotta appropriati siano implementati nel Gruppo al fine di mantenere i Dati Personali in modo accurato e aggiornato, tenendo in considerazione la quantità di dati raccolti, la velocità con la quale questi potrebbero cambiare e qualsiasi altro fattore rilevante;
- effettuare corsi di formazione regolari in materia di Protezione dei Dati, dare spiegazioni in merito ad argomenti e questioni correlati;
- informare e consigliare il Gruppo e i dipendenti che svolgono il trattamento sui loro obblighi in conformità al presente Codice;
- monitorare la conformità al presente Codici e effettuare degli *audit*;;
- fornire consulenza quando richiesto per quanto riguarda la valutazione d'impatto della Protezione dei Dati Personali e monitorare la performance;
- controllare e analizzare cambiamenti nella legislazione applicabile;
- riesaminare i tempi di conservazione di tutti i Dati personali trattati dal Gruppo e identificare qualsiasi dato che non è più necessario nell'ambito della finalità per la registrazione;

- adottare le misure opportune quando una controparte trasmette dei dati personali imprecisi o non aggiornati, per comunicare loro che l'informazione è imprecisa e/o non aggiornata e non può essere utilizzata per comunicare decisioni circa gli interessati; e per comunicare qualsiasi correzione dei Dati Personali alla controparte laddove sia richiesto;
- considerare la portata del possibile danno o perdita che potrebbe essere arrecato a soggetti (es. dipendenti o controparti) se si verifica una violazione della sicurezza, l'effetto di qualsiasi violazione della sicurezza a danno del Gruppo stesso, e qualsiasi danno di reputazione inclusa la possibile perdita di fiducia del cliente.

Responsabile UE della Protezione dei Dati

Il Responsabile UE della Protezione Dati deve essere residente nella UE e deve essere nominato sulla base di qualità professionali e, in particolare, per la conoscenza approfondita della legislazione e delle pratiche in materia di Protezione dei Dati e alla capacità di adempiere ai seguenti doveri:

- collaborare con le autorità di vigilanza UE, il Responsabile Globale della Protezione dei Dati e i Responsabili Locali della Protezione Dati (se nominati);
- agire come referente nei confronti delle autorità di vigilanza su questioni riguardanti il trattamento dei dati e le violazioni dei dati;
- monitorare e analizzare i cambiamenti nella legislazione UE e comunicare tali variazioni ai Responsabili Globali della Protezione dei Dati.

Responsabile Locale della Protezione dei Dati

Ciascun membro del Gruppo può incaricare un Responsabile Locale della Protezione dei Dati affinché assista i Responsabili Globali e UE della Protezione dei Dati nello svolgimento delle succitate mansioni.

5. *Governance* relativa al presente Codice

5.1. Responsabilità

Ciascun membro del Gruppo è l'unico responsabile della conformità al presente Codice, ai relativi obblighi legali e al trattamento appropriato dei dati personali. La conformità ai requisiti del Codice è obbligatoria per i dipendenti impegnati nei processi.

Se vi sia motivo di credere che gli obblighi legislativi contraddicano gli obblighi del presente Codice in materia di Protezione dei Dati Personali, il membro del Gruppo deve informare il Responsabile Globale della Protezione dei Dati. Nell'eventualità di conflitto tra la normativa nazionale e il Codice, il Gruppo lavorerà con il membro del Gruppo pertinente per trovare una soluzione pratica che soddisfi gli scopi del Codice in materia di Protezione dei Dati Personali.

Se ritenuto opportuno, un membro del Gruppo può adottare norme complementari o devianti in relazione al presente Codice. Queste norme devono essere approvate dal Responsabile Globale della Protezione dei Dati del Gruppo.

5.2. Controlli

Ciascun membro del Gruppo garantisce che l'ottemperanza ai requisiti del Codice o l'avviso di qualsiasi violazione, che potrebbe essere già accaduta o che possa potenzialmente accadere, non possa comportare conseguenze negative per il dipendente interessato. Nel contempo il Gruppo non accetterà alcuna azione da parte dei dipendenti che possa violare il Codice.

Il Gruppo presume e si aspetta che tutti i dipendenti riferiscano qualsiasi caso di violazione o potenziale violazione del Codice attraverso la "linea per la segnalazione di violazioni" (Whistleblowing line). Dettagli sulla linea sono di pubblico dominio e sono pubblicate sul portale aziendale.

Il Gruppo si riserva il diritto di controllare periodicamente la conoscenza in materia di Protezione dei Dati Personali da parte dei dipendenti, verificare la performance e l'esecuzione del presente Codice e di realizzare un'analisi della sua efficacia.

5.3. Riservatezza

Come descritto nel paragrafo 4.4, i Dati Personali sono soggetti a obblighi di riservatezza.

Tuttavia, in alcune circostanze, è consentito che i dati personali siano condivisi senza la conoscenza o il consenso dell'interessato. Questo è il caso in cui la divulgazione di Dati personali sia necessaria per qualsiasi dei fini seguenti:

- La prevenzione e l'accertamento di un crimine.
- L'arresto o il procedimento penale contro criminali.
- La valutazione o la riscossione di una tassa o tributo.
- Su ordine di un tribunale o in accordo con qualsiasi norma di legge.

Se qualsiasi membro del Gruppo tratta dei dati personali per uno di queste finalità, è possibile applicare un'eccezione all'obbligo di riservatezza, ma soltanto nella misura in cui l'omissione probabilmente pregiudicherebbe il caso in questione.

Se qualsiasi membro del Gruppo riceve richiesta da un tribunale o da qualsiasi autorità di regolamentazione o giudiziaria in merito a informazioni relative ad una persona interessata, l'organizzazione deve immediatamente informare il Responsabile Globale della Protezione dei Dati che fornirà guida e assistenza universale.

5.4. Riesame del Codice

Il presente Codice sarà riesaminato periodicamente dal Responsabile Globale della Protezione dei Dati, ma almeno annualmente, al fine di garantire che il Codice sia aggiornato e in linea con tutte le leggi e legislazioni applicabili.

Qualsiasi modifica sarà notificata immediatamente al Gruppo che implementerà le modifiche.

L'ultima versione della *Policy* in materia di Protezione dei Dati può essere consultata sul sito web del Gruppo: www. eurochemgruppo.com

5.5. Reclami e domande

Tutte le domande relative al presente Codice e ai suoi allegati possono essere inviate al Responsabile Globale della Protezione dei Dati o al pertinente Responsabile Locale della Protezione dei Dati.

Le persone interessate che debbano presentare reclamo riguardo al trattamento dei propri dati personali, lo devono fare per iscritto al Responsabile Globale della Protezione dei Dati. Un accertamento sul reclamo sarà eseguito nella misura in cui è appropriato in base al merito del caso specifico. Il Responsabile Globale della Protezione dei Dati informerà l'interessato sul progresso e risultato del reclamo entro un periodo ragionevole.

Se la questione non può essere risolta attraverso la consultazione tra la persona interessata e il Responsabile Globale della Protezione dei Dati, allora l'interessato potrà, a sua discrezione, cercare rimedio attraverso mediazione, arbitrato vincolante, contenzioso o denuncia presso la pertinente Autorità di Protezione dei Dati all'interno della giurisdizione applicabile.

Allegato 1. Riferimenti

	ID	Titolo del documento	Note
Documento normativo			
1		Codice di Condotta Compliance EuroChem Group AG	
2		Codice di Condotta EuroChem Group AG	
3		Legge Federale sulla Protezione Dati (FADP)	

Allegato 2. Registro delle violazioni dei dati

№	Membro del Gruppo	Categoria dei dati personali	Descrizione	№ di persone interessate coinvolte	Recapiti delle persone interessate	Potenziali conseguenze	Misure intraprese/da intraprendere

Allegato 3. Piano di conservazione

№	Membro del Gruppo	Categoria di dati personali	Tipo di registrazione	Periodo di conservazione

Allegato 4. Registro dei dati

№	Membro del Gruppo*	Categoria e descrizione dei dati personali*	Finalità del trattamento*	Categorie di destinatari*	Trasmissione a terzi	Limiti di tempo per la cancellazione	Misure di sicurezza

Le colonne contrassegnate con * sono campi obbligatori.