ELIOR-GRUPPE

Richtlinie zum Schutz personenbezogener Daten

Bereich	Alle Bereiche
Version	V1
Redakteur	pbD-Arbeitsgruppe
Prüfer	pbD-Lenkungsausschuss
Datum der Veröffentlichung	01.03.2019
Datum der Aktualisierung	

Einleitung

Diese Richtlinie zum Schutz personenbezogener Daten legt fest, wie die Elior-Gruppe bei der Verarbeitung personenbezogener Daten vorgeht, um den Schutz der Grundrechte und -freiheiten natürlicher Personen, insbesondere ihres Rechts auf Schutz personenbezogener Daten, zu gewährleisten.

Sie definiert die Standards, die alle Mitarbeiter, Mitarbeiterinnen, Partner und Subunternehmer der Elior-Gruppe bei der Verarbeitung personenbezogener Daten beachten müssen.

Es wird darauf hingewiesen, dass die Elior-Gruppe bei Nichteinhaltung der Verpflichtungen zum Schutz personenbezogener Daten mit einer Strafe von 4% ihres weltweiten Umsatzes belegt wird; dies entspricht indikativ fast 268 Mio. € auf der Grundlage des Betriebsergebnisses des Geschäftsjahres zum 30. September 2018.

Jede betroffene Person hat insbesondere auf folgendes zu achten:

- die Einhaltung des Grundsatzes des Schutzes der Privatsphäre bereits in der Entwurfsphase neuer Projekte (*privacy by design*), insbesondere dass jeder Datenverarbeitungsvorgang (i) einem bestimmten Zweck entspricht, (ii) die Unterrichtung von Personen über den durchgeführten Datenverarbeitungsvorgang vorsieht, (iii) Schutzmaßnahmen festlegt und (iv) eine Aufbewahrungsfrist für personenbezogene Daten festlegt;
- die Einhaltung der gesetzten Fristen für die Beantwortung von Anträgen auf Ausübung von Rechten, nämlich einen Monat, und Mitteilung von Datenlecks an die zuständigen Behörden innerhalb von 72 Stunden;
- ganz allgemein, auf die Einhaltung der durch diese Richtlinie eingeführten Prozesse und Empfehlungen sowie gegebenenfalls die Aufforderung an die Verantwortlichen für den Schutz personenbezogener Daten oder das DSGVO-Team der Elior-Gruppe unter gdpr-contact@eliorgroup.com.

GLOSSAR

„**Elior-Gruppe**“ bezeichnet die Gesellschaft Elior Group und alle Gesellschaften die, im Sinne des Artikels L233-3 des französischen Handelsgesetzbuches,

(i) unter direkter oder indirekter Kontrolle der Gesellschaft Elior Group stehen, oder,

(ii) Direkt oder indirekt unter gemeinsamer Kontrolle mit der Gesellschaft Elior Group stehen;

„**personenbezogene Daten**“, „**persönliche Daten**“ oder auch „**pbD**“ bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (im Folgenden „**Betroffener**“). Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

„**Datenverarbeitung**“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

„**Verantwortlicher**“ bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

„**Auftragsverarbeiter“** bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

„**SI Verantwortlicher**“ bezeichnet den Mitarbeiter innerhalb der Elior-Gruppe, der für das technische Wissen über die an der Verarbeitung beteiligten IT-Ressourcen für jede innerhalb der Elior-Gruppe identifizierte pbD-Verarbeitung verantwortlich ist;

„**Betrieblich Verantwortlicher**“ bezeichnet den Mitarbeiter innerhalb der Elior-Gruppe, der die betriebliche Notwendigkeit und den Zweck (Geschäftsleitung) der Verarbeitung definiert, und zwar für jede innerhalb der Elior-Gruppe identifizierte Datenverarbeitung;

„**Empfänger**“ bezeichnet eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob dieser Empfänger Externer der Elior-Gruppe ist oder nicht (Dritter). Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

„**Einwilligung [der betroffenen Person]**“ bezeichnet jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

„**Verletzung des Schutzes personenbezogener Daten**“ bedeutet eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

„**verbindliche interne Datenschutzvorschriften**“ oder „**Binding Corporate Rules**“ oder „**BCR**“ bezeichnet eine konzerninterne Datenschutzrichtlinie im Zusammenhang mir der Übermittlung personenbezogener Daten, die ganz oder teilweise außerhalb des Europäischen Wirtschaftsraums erfolgt. Sie sind rechtsverbindlich und

werden von den Unterzeichnern einer Unternehmensgruppe, unabhängig vom Land ihrer Niederlassung, sowie von allen Mitarbeitern derselben juristischen Person oder Unternehmensgruppe respektiert. Es gibt zwei Arten von BCR: (i) die BCR

„Verantwortlicher", die es ermöglichen, Übertragungen innerhalb einer als Verantwortlicher fungierenden Gruppe zu überwachen, und (ii) die BCR „Auftragsverarbeiter", die es ermöglichen, eine sichere Umgebung für Übertragungen zu schaffen, wenn die Gruppe als Auftragsverarbeiter auftritt;

„**Datenschutz-Folgenabschätzung**" oder „**Data Protection Impact Assessment**" oder „**DSFA**" bedeutet, dass der Verantwortliche, vor einer Verarbeitung, die, insbesondere bei Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführt. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Inhaltsverzeichnis

1. Kontext

Als Catering-Dienstleister ist die Lebensmittelsicherheit ein wesentlicher Aspekt des Geschäfts der Elior-Gruppe. Das Angebot gesunder Lebensmittel, die nach den geltenden Richtlinien für Kunden und Gäste zubereitet und geliefert werden, ist ein ständiges Anliegen der Elior-Gruppe und eine der Grundlagen für das Vertrauen, das sie ihr entgegenbringen. Ebenso stellt die gesetzeskonforme Verarbeitung personenbezogener Daten eine wesentliche Herausforderung für die Elior-Gruppe dar.

Der rasante technologische Wandel und die Globalisierung haben in der Tat zu einer erheblichen Zunahme des Austauschs personenbezogener Daten zwischen den Beteiligten geführt, was zu neuen Herausforderungen für den Schutz von pbD geführt hat. Der Umfang der Erhebung und die Weitergabe personenbezogener Daten hat erheblich zugenommen, was zu einer beispiellosen Nutzung und Aufwertung dieser Daten führt. Die Elior-Gruppe hat den Anspruch, sich durch technologische Innovationen im digitalen Bereich und eine zunehmende Fähigkeit zur Datenerhebung und -nutzung zu differenzieren und folgt diesem Trend voll und ganz. Daten sind allgegenwärtig und stehen heute im Mittelpunkt der Wertschöpfungskette. Gut verwaltet und geschützt, verbessern sie Effizienz und Wettbewerbsfähigkeit, personalisieren und stärken die Beziehungen zu Kunden und Gästen, erobern neue Märkte, verbessern Produkte und Dienstleistungen und erleichtern die Zusammenarbeit und Mobilität.

Dies kann nicht ohne das Vertrauen geschehen, das es der Elior-Gruppe ermöglicht, ihre digitale Positionierung zu entwickeln, indem sie Teams, Kunden, Gästen und ganz allgemein allen Partnern der Elior-Gruppe die Kontrolle über die sie betreffenden personenbezogenen Daten garantiert.

Angesichts der entstandenen nationalen und supranationalen gesetzlichen Rahmenbedingungen passt sich die Elior-Gruppe ständig den Herausforderungen der Digitaltechnik an und entwickelt einen Ansatz zur kontinuierlichen Verbesserung und Einhaltung der Vorschriften für den Umgang mit personenbezogener Daten.

2. Bereich

Die Elior-Gruppe verarbeitet im Rahmen ihrer Tätigkeit ständig personenbezogene Daten, wie z. B.:

- bei der Bildaufnahme mit Videoüberwachungskameras;
- Bei der Bearbeitung von Kundenanfragen;
- bei der Erfassung der Diäten der Gäste, um ihnen angemessene Mahlzeiten servieren zu können.;
- oder bei der Sammlung von Informationen über die Teams im Rahmen ihres Karrieremanagements.

Diese Richtlinie gilt für alle Mitarbeiter, Mitarbeiterinnen, Subunternehmer, Subunternehmerinnen und Partner der Elior-Gruppe, wann immer personenbezogene Daten von Kunden, Gästen, Teams, Lieferanten oder anderen Personen erhoben, verwendet, zugänglich gemacht oder weitergegeben werden.

Angesichts des Sitzes der Elior-Gruppe in Frankreich zielt diese Richtlinie insbesondere darauf ab, die Verpflichtungen aus der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr dieser Daten, nachstehend "Datenschutz-Grundverordnung", "Verordnung" oder "DSGVO" genannt, zu erfüllen.

Dieser Ansatz ist Teil des Bestrebens, die Praktiken innerhalb der Elior-Gruppe von oben zu harmonisieren, die Überwachung und Aufrechterhaltung der Einhaltung im Laufe der Zeit zu vereinfachen und ein hohes Schutzniveau für personenbezogene Daten zu gewährleisten. Um dieses Ziel zu erreichen, muss diese Richtlinie so weit wie möglich die nationalen Besonderheiten berücksichtigen:

- innerhalb des Europäischen Wirtschaftsraumes gemäß der Datenschutz-Grundverordnung, unter Einhaltung spezifischer nationaler Rechtsvorschriften, die die Bedingungen festlegen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist;
- außerhalb des Europäischen Wirtschaftsraums, in allen Staaten, in denen die Elior-Gruppe präsent ist, unter Berücksichtigung der jeweiligen nationalen Rechtsvorschriften zum Schutz personenbezogener Daten, oder sogar einer für ihre Anwendung speziell zuständigen Behörde.

Es sollte klargestellt werden, dass das Recht auf Schutz personenbezogener Daten kein absolutes Recht ist, sondern im Hinblick auf seine Funktion in der Gesellschaft zu sehen ist und mit anderen Grundrechten, im Einklang mit dem Grundsatz der Verhältnismäßigkeit abgewogen werden muss, insbesondere der Achtung der Privat- und Familiensphäre, des Haushalts und der Kommunikation, der Gedanken-, Gewissens- und Religionsfreiheit, der Meinungs- und Informationsfreiheit sowie der Unternehmensfreiheit. Diese Politik zielt nicht darauf ab, das Gleichgewicht zwischen diesen Rechten zu definieren, das von den Rechtsabteilungen der Elior-Gruppe im Hinblick auf die Entwicklung der Rechtsprechung und die Empfehlungen der Behörden von Fall zu Fall geprüft werden muss.

3. Governance

A. Allgemeiner Rahmen

Der Kontrollprozess des Datenmanagements wird von einem **Konzernteam** geleitet, das sich zusammensetzt aus:

- Einem **Group Chief Compliance Officer**: dem Generaldirektor direkt unterstellt, ist er verantwortlich für die Umsetzung der Compliance-Regeln. Es ist der Garant für die Einhaltung eines optimalen Schutzniveaus der personenbezogenen Daten innerhalb der Elior-Gruppe;

- Einem **Group Data Protection Officer** (DPO): Er ist der Garant für die Umsetzung des Programms zum Schutz personenbezogener Daten und der Anwendung der einschlägigen Gesetze in der gesamten Elior-Gruppe. Er verfügt über gute Kenntnisse der Tätigkeiten und der Organisation der Elior-Gruppe, insbesondere der Verarbeitungsvorgänge, der Informationssysteme und der Bedürfnisse der Elior-Gruppe in Bezug auf Datenschutz und Sicherheit. Er übt seine Funktion vollkommen unabhängig aus und wird unterstützt von einem **Group IT Security Compliance Manager**.

- Einem **Group Senior Legal Counsel**: Er unterstützt und berät den DPO beim Verständnis und der Interpretation von Gesetzestexten und in den Beziehungen zu den Behörden für den Schutz personenbezogener Daten. Er sorgt auch für die Berücksichtigung der Problematiken des Schutzes personenbezogener Daten in den Vertragsbeziehungen.

Das Konzernteam wird von dezentralen Akteuren in der Elior-Gruppe unterstützt: den **DCP-Botschaftern**. Diese DCP-Botschafter sind die Vermittler des DPO in ihrem Bereich und tragen namentlich dazu bei:

- Richtlinien und damit verbundene verfahren auszuarbeiten;
- die Einhaltung der Konzernrichtlinie sicherzustellen, insbesondere in Bezug auf die Ausübung von Rechten und die Führung des Verarbeitungsverzeichnisses;
- die bevorzugten Ansprechpartner für das DSGVO-Team der Gruppe und deren Umfeld für alle Fragen im Zusammenhang mit pbD zu sein.

Diese Richtlinie wird auf Initiative des DSGVO-Teams der Gruppe jährlich überprüft, um Änderungen in der Gesetzgebung oder internen Praktiken innerhalb der Elior-Gruppe zu berücksichtigen. Es steht den Tochtergesellschaften der Elior-Gruppe frei, wie sie sich intern organisieren, um diese Richtlinie anzuwenden und ihre Verbreitung und Anwendung zu erleichtern.

B. Konformitätswerkzeug

Die Elior-Gruppe hat kürzlich eine Compliance-Management-Software erworben, um den Verpflichtungen zum Schutz personenbezogener Daten nachzukommen und die damit verbundenen Verfahren zu verwalten und ihre Teams bei der Einhaltung der Compliance-Regeln im Rahmen ihrer Aktivitäten zu unterstützen.

Alle Mitarbeiter der Elior-Gruppe, die für die Verarbeitung personenbezogener Daten verantwortlich sind (d.h. IT-Verantwortliche und Geschäftsleitung sowie DCP-Botschafter), haben Zugang zu dieser Umgebung. Dieses Tool ermöglicht insbesondere:

- die Pflege der Verarbeitungsverzeichnisse (Verantwortlicher/Auftragsverarbeiter);
- Unterstützung der Projektleiter bei der Umsetzung von Datenschutzanforderungen;
- Kontaktformulare von Personen für die Ausübung der Rechte zu erstellen und deren Verarbeitung verwalten;
- Die Pflege eines Verzeichnisses der Auftragsverarbeiter;
- Die Erstellung von Mitteilungen über Zwischenfälle;
- generell, die Einhaltung der Gesetze innerhalb der Elior-Gruppe im Einklang mit dem Prinzip des Verantwortungsbewusstseins sicherzustellen.

Es liegt jedoch in der Verantwortung:

- der Projektleiter (IT-Verantwortliche und Geschäftsleitung), über jede neue Datenverarbeitung in diesem Umfeld informieren, und der pbD-Botschafter, Unterstützung zu leisten und die bereitgestellten Informationen zu validieren;
- der pbD-Botschafter, mit Unterstützung von IT- und Geschäftsleitung die ordnungsgemäße Bearbeitung von Anträgen zur Ausübung von Rechten zu überwachen.

C. pbD-Lenkungsausschuss (pbD-LA)

Der Lenkungsausschuss für personenbezogene Daten ist unter Leitung des DPO und dem Vorsitz des Group Chief Compliance Officer die Entscheidungsinstanz.

Er hat insbesondere folgende Befugnisse in Bezug auf den Schutz personenbezogener Daten innerhalb der Elior-Gruppe:

- die Richtlinien und ihre Entwicklung zu kontrollieren;
- Erstellung des Jahresberichts über die Maßnahmen;
- den Grad der Einhaltung festzuhalten;
- die Priorität von Maßnahmen zu prüfen und zu beurteilen.

Zusätzlich zum Gruppenteam setzt sich der pbD-LA aus folgenden Mitgliedern zusammen:

- dem IT-Direktor der Gruppe;
- dem Direktor der Rechtsabteilung der Gruppe;
- dem Direktor für internes Audit der Gruppe;
- dem Direktor Versicherungen und Risikoprävention der Gruppe;
- den IT-Direktoren der Unternehmen;
- den Direktoren der Rechtsabteilungen der Unternehmen.

Eine Sammlung der Entscheidungen des pbD-LA's wird durch den DPO nach den Ausschüssen systematisiert. Die Protokolle sind für alle Beteiligten zugänglich.

Der pbD-LA tritt jährlich zusammen. Er kann auf Vorschlag des DPO aus besonderem Anlass auch außerordentlich zusammentreten (schwerer Zwischenfall, großes Schiedsverfahren, Kontrolle der Behörden usw.).

D. Arbeitsgruppe zum Schutz personenbezogener Daten (AG)

Der pbD-Arbeitsausschuss ist unter Leitung des IT Security Compliance Managers und dem Group Senior Legal Counsel und dem Vorsitz des DPO die Planungsinstanz und folgt den Empfehlungen des pbD-LA.

Neben dem Gruppenteam sind auch die pbD-Botschafter der Bereiche (Gemeinschaftsverpflegung, Konzessionsverpflegung und Dienstleistungen) und, je nach Bedarf, pbD-Botschafter im internationalen Umfeld vertreten.

Der AA-pbD tritt bei Bedarf zusammen.

E. Querverantwortung

Der IT Security Compliance Manager ist verantwortlich für die Leitung der Arbeiten zum Schutz personenbezogener Daten in Frankreich und international. Er hat auch die Aufgabe, die damit verbundenen guten Praktiken innerhalb der Elior-Gruppe zu identifizieren und zu verbreiten.

4. Unsere Pflichten

Dieser Abschnitt beschreibt die verschiedenen Pflichten in Verbindung mit dem Schutz personenbezogener Daten, die der Elior-Gruppe obliegen.

A. Verantwortung und Verarbeitungsverzeichnisse

Die Datenschutz-Grundverordnung führt den Grundsatz der Rechenschaftspflicht, oder *accountability*, im Bereich der Datenverarbeitung ein. Seit ihrem Inkrafttreten muss die Elior-Gruppe in der Lage sein, Ihre Konformität mit der Verordnung nachzuweisen; dies erfolgt insbesondere durch das eingeführte Verarbeitungsverzeichnis.

Daher müssen innerhalb der Elior-Gruppe zwei Arten von Verzeichnissen geführt werden; das erste betrifft Verarbeitungsvorgänge, für die ein Unternehmen der Elior-Gruppe Verantwortlicher ist, das zweite betrifft Verarbeitungsvorgänge, für die ein Unternehmen der Elior-Gruppe als Auftragsverarbeiter agiert.

Für jede Verarbeitung, für die die Elior-Gruppe Verantwortlicher ist, müssen die folgenden Informationen im Verzeichnis enthalten sein:

- die Identität des Verantwortlichen und der Auftragsverarbeiter;
- die Identität der IT- und Geschäftsleitung;

- der Zweck (das mit der Datenerhebung und -verarbeitung verfolgte Ziel);
- die Rechtsgrundlage der Verarbeitung;
- die Liste der erhobenen Daten, ihre Aufbewahrungsdauer und die betroffenen Personen;
- die Kategorien von Personen, die Zugang zu den Daten haben (Administrator, Personalwesen, Auftragsverarbeiter, usw.);
- Vorliegen einer Übertragung in ein Drittland;
- die Art, wie die Information der Personen realisiert wird;
- die eingesetzten Sicherheitsmaßnahmen;
- Eventuell die Ergebnisse der DSFA.

Für jede Verarbeitung, für die die Elior-Gruppe Auftragsverarbeiter ist, müssen die folgenden Informationen im Verzeichnis enthalten sein:

- der Name und die Kontaktdaten jedes Kunden, zu dessen Gunsten die Daten verarbeitet werden;
- gegebenenfalls der Name und die Kontaktdaten jedes weiteren Auftragsverarbeiters;
- die Kategorien der für jeden Kunden durchgeführten Verarbeitungen;
- die zugunsten des Kunden durchgeführten Datenübertragungen außerhalb der EU;
- nach Möglichkeit, eine allgemeine Beschreibung der eingerichteten technischen und organisatorischen Sicherheitsmaßnahmen.

Es liegt in der Verantwortung der IT- und Geschäftsleitung, dieses Verzeichnis mit Unterstützung ihrer pbD-Botschafter auszufüllen.

B. Transparenz und Treu und Glauben

Transparenz

Es ist die Pflicht der Elior-Gruppe und ihrer Teams, bei der Verarbeitung personenbezogener Daten klar und transparent zu sein. Die gesammelten Daten dürfen nicht in einer Weise und mit einer Absicht verwendet werden, die nicht vernünftigerweise erwartet werden kann und nicht für den beabsichtigten Zweck bestimmt ist.

Daher ist es vor der Erhebung personenbezogener Daten notwendig, folgendes in einer klaren und einfachen Sprache zu kommunizieren:

- wer wir sind;
- welche personenbezogenen Daten erhoben werden und aus welcher Quelle sie stammen;
- die Vorgänge, die mit den personenbezogenen Daten durchgeführt werden sollen und die Rechtsgrundlage;
- ob die personenbezogenen Daten aktuell oder in Zukunft mit weiteren Empfängern geteilt werden;
- die Aufbewahrungsdauer der personenbezogenen Daten;
- ob die personenbezogenen Daten nach außerhalb des Europäischen Wirtschaftsraums übermittelt werden;
- die Rechte, die Einzelpersonen bei der Verarbeitung personenbezogener Daten garantiert werden.

Rechtmäßigkeit der Verarbeitung

Damit die Verarbeitung personenbezogener Daten rechtmäßig ist, ist es notwendig, berechtigte Gründe zu haben, rechtliche Verpflichtungen zu begründen oder die Zustimmung der betroffenen Person einzuholen. Vor der Verarbeitung personenbezogener Daten ist daher neben der Information der Personen sicherzustellen, dass diese auf einer der folgenden Grundlagen beruhen:

- **Gesetzliche Verpflichtung**: die Verarbeitung ist notwendig, um einer rechtlichen Verpflichtung nachzukommen, welcher der für die Verarbeitung Verantwortliche unterliegt (nationales oder EU-Recht), z.B. die Übermittlung von Daten über die Vergütung der Arbeitnehmer an die Sozialversicherungs- und Steuerbehörden.

- **Vertragliche Notwendigkeit**: die Verarbeitung ist für die Erfüllung eines Vertrags, an dem die betroffene Person beteiligt ist, oder für die Durchführung von auf ihren Antrag getroffenen vorvertraglichen Maßnahmen erforderlich.
  Diese Situation darf sich nur auf Leistungen erstrecken, die für die Erfüllung des Vertrages wesentlich sind, wie z. B. die Erhebung der Kontaktdaten eines Gastes für die Bearbeitung und den Versand von Rechnungen oder die Verarbeitung von Mitarbeiterdaten für die Gehaltsabrechnung, nicht aber für irgendwelche kommerzielle Akquisition.

- **Berechtigte Interessen**: die Verarbeitung ist für die berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, es sei denn, es gelten die Interessen oder Grundrechte und -freiheiten des Betroffenen, die den Schutz personenbezogener Daten erfordern. Das berechtigte Interesse des Verantwortlichen muss dann systematisch gegen die Grundrechte und -freiheiten der Betroffenen abgewogen werden, z.B. die Übermittlung korruptionsbezogener Angaben an eine Behörde außerhalb der Europäischen Union oder die Analyse des Internetverkehrs, um den Zugang zu bösartigen Systemen zum Zwecke der Sicherheit der Computernetze zu verhindern.

- **Lebenswichtige Interessen**: die Verarbeitung ist notwendig, um die berechtigten Interessen des Betroffenen oder einer anderen natürlichen Person zu schützen, z.B. die Erhebung einer persönlichen Telefonnummer für den Versand von SMS-Benachrichtigungen bei schwerwiegenden Ereignissen am Arbeitsplatz oder die Erhebung von Daten über eine Diät, um eine Gefahr für die Gesundheit einer Person zu vermeiden.

- **Öffentliches Interesse**: Diese Rechtsgrundlage betrifft die Situation, in der der Verantwortliche von einer Behörde oder mit einer Aufgabe im öffentlichen Interesse betraut ist, für die eine Verarbeitung erforderlich ist. In diesem Fall ist diese Rechtsgrundlage von Fall zu Fall nach Überprüfung durch einen pbD-Botschafter anzuwenden.

- **Einholung der Zustimmung**: der Betroffene hat der Verarbeitung seiner personenbezogenen Daten für einen oder mehrere bestimmte Zwecke zugestimmt:
    - Seine Zustimmung muss frei (freie Wahl, ohne negative Folgen), konkret (eine konkrete Zustimmung für jeden Zweck), in informierter Weise (Vorhandensein geeigneter und ausreichender Informationen zum Zeitpunkt der Zustimmungserklärung) und unmissverständlich (Logik des "Opt-in", keine Unklarheiten und fehlende Zustimmung per Voreinstellung oder verknüpft mit Untätigkeit) sein;
    - die Zustimmung muss nachweisbar sein (z.B. Ankreuzfeld, auszufüllendes Formular, systematische Verfahren oder Mechanismen) und der Person die Möglichkeit geben, sie zu widerrufen.

Datenminimierung

Darüber hinaus müssen die gesammelten und aufgezeichneten Informationen für den verfolgten Zweck maßgeblich und unbedingt erforderlich sein. Daher müssen Maßnahmen ergriffen werden, um die Menge der erfassten personenbezogenen Daten zu minimieren und sicherzustellen, dass sie für die Zwecke der Verarbeitung angemessen sind.

C. Korrekte Daten pflegen und für einen begrenzten Zeitraum aufbewahren

Falsche oder ungenaue Informationen über eine Person können zu Schäden führen. So könnte beispielsweise eine Person von Leistungen oder Vorteilen, die sich aus ihrem Status ergeben, ausgeschlossen werden. Daher ist bei einer Entscheidung auf der Grundlage personenbezogener Daten besondere Vorsicht geboten.

Korrektheit von Daten

Die Mitarbeiter der Elior-Gruppe müssen die Richtigkeit der gespeicherten Informationen sicherstellen, insbesondere durch die Einrichtung der folgenden Verfahren:

- nach Möglichkeit die Richtigkeit der Informationen zum Zeitpunkt der Erhebung zu überprüfen;
- den Betroffenen so weit wie möglich die Möglichkeit zu geben, die sie betreffenden Daten zu aktualisieren;
- die gespeicherten personenbezogenen Daten regelmäßig zu überprüfen, um sicherzustellen, dass sie auf dem neuesten Stand sind;
- unrichtige Daten zu korrigieren oder zu löschen.

Risiken, die mit freien Kommentarbereichen (ZLCs) verbunden sind

Besondere Sorgfalt ist bei Textfeldern und Kommentarbereichen geboten. Diese freien Textfelder sind nützlich, um die Verfolgung eines Falls sicherzustellen oder eine Beziehung zu personalisieren. Ihre Verwendung ist zwar nicht verboten, aber Sensibilisierungsmaßnahmen und Verwaltungsvorschriften müssen ihre Verwendung regeln, um zu verhindern, dass die eingegebenen Kommentare die Rechte der Betroffenen verletzen.

Einige Kommentare können abwertend, diskriminierend oder sogar beleidigend sein oder sogenannte sensible Daten wie Gesundheitsdaten offenlegen. Die Kommentare müssen daher angemessen, objektiv und respektvoll sein.

Die beste Vorkehrung ist, wenn man im Auge behält, dass die Betroffenen (Kunden, Gäste, Mitarbeiter usw.) jederzeit und auf einfache Anfrage von ihrem Zugangsrecht Gebrauch machen und auf den Inhalt dieser Kommentarbereiche zugreifen können.

Aufbewahrungsdauer

Personenbezogene Daten können nicht auf unbestimmte Zeit gespeichert werden, daher muss eine Aufbewahrungsfrist entsprechend dem Zweck festgelegt werden, für den die Daten erhoben wurden. Nach Erreichung dieses Ziels müssen diese Daten, je nach Fall, archiviert, gelöscht oder anonymisiert werden (insbesondere zur Erstellung von Statistiken).

Es ist wichtig zu beachten, dass diese Daten im berechtigten Interesse der Elior-Gruppe und der Verteidigung ihrer Interessen jedoch für längere Zeiträume aufbewahrt werden können, die durch einen bestimmten Kontext gerechtfertigt sind, z.B. im Rahmen von Rechtsstreitigkeiten, und zwar in allen Fällen nach Mitteilung an den DPO.

D. Gewährleistung der Datensicherheit

Die Sicherheit der Daten ist ein äußerst wichtiges Thema für die Elior-Gruppe. Wenn die Sicherheit der Daten über ihren gesamten Lebenszyklus nicht gewährleistet ist, von der Datenerhebung bis zur Vernichtung, kann dies zu erheblichen Schäden für den Einzelnen führen. Die Sicherheit externer Anbieter, die an einer Verarbeitung personenbezogener Daten beteiligt sind, muss strikt überwacht werden.

Es gibt viele Möglichkeiten, personenbezogene Daten, sei es in elektronischer oder in gedruckter Form, zu schützen. Um ihre Mitarbeiter zu informieren, stellt ihnen die Elior-Gruppe ein Dokumentenregister zur Verfügung, das den neuesten Anforderungen entspricht und dessen Anwendung obligatorisch ist:

- eine Sicherheitspolitik der Informationssysteme und entsprechende Richtlinien, in denen die Anforderungen an die Informationssysteme der Elior-Gruppe aufgeführt sind;
- Sicherheitsanforderungen, die eine Voraussetzung für jeden Vertrag mit einem IT-Dienstleister sind.

Die nachstehenden Empfehlungen werden von Fall zu Fall und entsprechend den Risiken der Datenverarbeitung für die Freiheiten und die Privatsphäre der betroffenen Personen angepasst:

- Anwendungen müssen durch Authentifizierungssysteme (Benutzername und Passwort) entsprechend der Informationssicherheitspolitik geschützt werden;
- der Zugang zu den personenbezogenen Daten ist nur Personen gestattet, die zum Zugang zu den betreffenden Daten befugt sind, es handelt sich um das „Need-to-know-Prinzip“;
- unabhängig von der Art des physischen Mediums, digitales oder Papierformat, müssen diese gesichert werden. Bei mobilen Geräten ist besondere Vorsicht geboten, und diese Geräte dürfen nicht unbeaufsichtigt oder ungeschützt sein.

Bei Fragen können Sie sich an den IT-Sicherheitsbeauftragten der Elior-Gruppe wenden.

E. Auftragsverarbeitung und Übermittlung personenbezogener Daten

Im Falle einer Übermittlung personenbezogener Daten muss die Elior-Gruppe zunächst sicherstellen, dass dies rechtlich möglich und sicher ist. Die Übermittlung personenbezogener Daten ist im weitesten Sinne zu verstehen, wie es beispielsweise der Fall sein kann:

- bei Datenübermittlungen selbst zwischen juristischen Personen innerhalb der Elior-Gruppe;
- bei einer ausgelagerten Verwaltung oder Wartung einer IT-Ressource;
- beim Hosting eines Dienstes in der Cloud.

Pflichten des Auftragsverarbeiters

Gemäß der DSGVO ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen bei seinem permanenten Compliance-Prozess zu unterstützen. Es obliegt dem Verantwortlichen, sicherzustellen, dass der Auftragsverarbeiter diese Aufgabe erfüllt. Vom Auftragsverarbeiter muss die Verpflichtung zu folgendem erwartet werden können:

- **Transparenz**: ermöglicht durch die Ausarbeitung eines Rechtsakts (i), in dem die Verpflichtungen jeder Partei klar definiert sind, (ii) festgelegt wird, dass der Auftragsverarbeiter nur auf Anweisung des

Verantwortlichen handelt. Diese Transparenz wird auch dadurch gewährleistet, dass ein aktuelles Verzeichnis der im Auftrag des Verantwortlichen ausgeführten Tätigkeiten geführt wird und dass alle Informationen zur Verfügung gestellt werden, die zum Nachweis der Einhaltung dieser Verpflichtungen erforderlich sind;

- **Beratung und Unterstützung:**: der Auftragsverarbeiter muss den Verantwortlichen bei der Bestimmung der unbedingt erforderlichen Daten, bei der Bearbeitung von Anträgen auf Ausübung von Rechten und ganz allgemein bei allen seinen Verpflichtungen unterstützen;
- **Sicherheit**: der Auftragsverarbeiter muss sicherstellen, dass seine Mitarbeiter zur Vertraulichkeit verpflichtet sind, und alle Maßnahmen ergreifen, um ein den Risiken angemessenes Sicherheitsniveau und eine Speicherung der Daten ausschließlich für die vorgesehene Dauer zu gewährleisten;
- **Benachrichtigung**: der Auftragsverarbeiter muss den Verantwortlichen über jede Datenschutzverletzung innerhalb eines angemessenen Zeitraums (idealerweise 24 oder 36 Stunden) informieren.

Die Elior-Gruppe und ihre Teams verpflichten sich, sicherzustellen, dass diese Anforderungen für jeden Einsatz von Auftragsverarbeitern und wenn die Elior-Gruppe als Auftragsverarbeiter auftritt, erfüllt werden.

Wenn die Elior-Gruppe als Verantwortlicher auftritt und einen oder mehrere Auftragsverarbeiter einsetzt, muss dieser bzw. müssen diese die Anforderungen der Elior-Gruppe an den Schutz personenbezogener Daten erfüllen. Die Datenübermittlung an Subunternehmer muss auf sichere Weise erfolgen. Es liegt in der Verantwortung der Elior-Gruppe sicherzustellen, dass ihre Auftragsverarbeiter angemessene Maßnahmen zur Gewährleistung der Sicherheit personenbezogener Daten getroffen haben.

Die Rechtsabteilungen müssen systematisch konsultiert werden, um sicherzustellen, dass jeder Vertrag die erforderlichen Verpflichtungen zum Schutz personenbezogener Daten enthält.

Sonderfall der Übermittlung außerhalb des Europäischen Wirtschaftsraums (EWR):

Die Übermittlung personenbezogener Daten außerhalb des EWR muss durch geeignete Maßnahmen beschränkt werden, z. B.:

- die Vereinbarung von Vertragsklauseln, die von der Europäischen Kommission anerkannt sind;
- die Abfassung von verbindlichen Datenschutzvorschriften: BCR-“Verantwortlicher“ oder BCR-“Auftragsverarbeiter“;
- die Unterzeichnung spezieller Verpflichtungen (z. B.: Datenschutzschild) für Stellen außerhalb des EWR.

F. Ausübung der Rechte

Die Elior-Gruppe stellt sicher, dass die betroffenen Personen ihre Rechte in vollem Umfang wahrnehmen können, vor allem:

- den Zugriff auf die eigenen personenbezogenen Daten;
- die Berichtigung der personenbezogenen Daten zu verlangen;
- die Übertragbarkeit der personenbezogenen Daten in einem maschinenlesbaren Format zu verlangen;
- Widerspruch dagegen einzulegen, dass eine Entscheidung getroffen wird, die ausschließlich auf automatisierter Verarbeitung beruht;;
- die Löschung der personenbezogenen Daten zu verlangen;
- die Einschränkung der Verarbeitung der personenbezogenen Daten zu verlangen;
- der Verarbeitung personenbezogener Daten zu widersprechen.

G. Privacy by design

Es ist einfacher und kostengünstiger, Aspekte der Privatsphäre und Sicherheit so früh wie möglich in Projekten zu berücksichtigen. Deshalb liegt es von Anfang an in der Verantwortung des Projektleiters, die Fragen des Schutzes personenbezogener Daten zu berücksichtigen und die Privatsphäre der betroffenen Personen zu wahren, sei es bei der Umsetzung einer neuen Dienstleistung oder eines neuen Produkts oder bei deren Änderung.

Das bedeutet insbesondere, der Projektleiter muss bei jedem neuen Projekt:

- die möglicherweise vorhandenen personenbezogenen Daten identifizieren;
- gegebenenfalls:

- dieses Projekt in das Management-Tool zum Schutz personenbezogener Daten eingeben und den Anweisungen folgen,
- die Hauptrisiken im Zusammenhang mit personenbezogenen Daten ermitteln, die im Rahmen eines bestimmten Projekts auftreten können, einschließlich rechtlicher, Reputations- und persönlicher Risiken,
- für hochriskante Verarbeitungsvorgänge eine Datenschutz-Folgenabschätzung („DFSA") durchführen. Diese Verarbeitungen betreffen insbesondere die groß angelegte Verwendung von Daten, den Einsatz neuer Technologien, die Verarbeitung sensibler Daten, die systematische Überwachung oder die Durchführung von Verarbeitungen zur automatisierten Entscheidungsfindung und Profiling. Der Europäische Datenschutzausschuss bezieht sich auf seiner Website auf die Liste der Verarbeitungen, für die eine DSFA obligatorisch ist, und zwar von Land zu Land,
- die Einhaltung der Konzernrichtlinie sicherstellen,
- die Umsetzung und Kontrolle der organisatorischen und technischen Schutzverfahren überwachen.

Im Falle von Unterstützungs- oder Klärungsbedarf kann sich der Projektleiter an seine DCP-Botschafter wenden.

H. Kommunikation und Sensibilisierung

Jährlich wird in Abhängigkeit von den identifizierten Themen und den Feststellungen zur Compliance der Elior-Gruppe vom Konzernteam mit Unterstützung der DCP-Botschafter ein Kommunikations- und Sensibilisierungsplan initiiert. Ziel dieses Ansatzes muss es sein, innerhalb der Elior-Gruppe eine Kultur des Schutzes personenbezogener Daten zu schaffen.

Die Teams sind eingeladen, zur Verbesserung der Richtlinie und der damit verbundenen Prozesse beizutragen.

I. Besondere Kategorien der Verarbeitung und personenbezogener Daten

Sensible oder ähnliche personenbezogene Daten

Dies sind Informationen, die die rassische oder ethnische Herkunft, politische, philosophische oder religiöse Ansichten, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben einer natürlichen Person offenbaren. Hierzu gehören auch Informationen über Straftaten oder Verurteilungen.

Da diese Daten ein hohes Risiko für die Privatsphäre der Personen darstellen, wird empfohlen, dass die Elior-Gruppe sie nicht sammelt oder verwendet, außer in bestimmten Einzelfällen:

- wenn der Betroffene seine ausdrückliche Zustimmung (schriftlich, klar und ausdrücklich) erteilt hat;
- wenn die Daten für medizinische Zwecke oder für die Gesundheitsforschung erforderlich sind;
- wenn ihre Verwendung von der Behörde für den Schutz personenbezogener Daten genehmigt ist.

Da diese Fälle je nach nationalem Recht des Landes unterschiedlich sein können, ist es ratsam, sich bei dieser Art von Problemen an die DCP-Botschafter oder das DSGVO-Team der Gruppe zu wenden. Es muss eine systematische DSFA durchgeführt werden.

Personenbezogene Daten und Bildrechte bei Kindern

Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da sie sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind.

Im Rahmen der Dienste der Informationsgesellschaft ist die Verarbeitung personenbezogener Daten eines Kindes rechtmäßig, wenn das Kind mindestens 16 Jahre alt ist. Ist das Kind unter 16 Jahren alt, so ist diese Verarbeitung nur zulässig, wenn und soweit die Zustimmung des Inhabers der elterlichen Verantwortung für das Kind erteilt oder genehmigt wird. Die Mitgliedstaaten können zu diesem Zweck gesetzlich ein niedrigeres Alter vorsehen, sofern dieses Alter nicht unter 13 Jahren liegt. Zögern Sie nicht, den DCP-Botschafter zu kontaktieren, um die Altersgrenze für die beabsichtigte Verarbeitung festzulegen.

Vor der Durchführung dieser Verarbeitungen muss eine systematische DSFA durchgeführt werden.

Marketingmaßnahmen

Bei der Vermarktung müssen die Entscheidungen und Rechte der betroffenen Personen beachtet werden. Bei Marketingmaßnahmen, insbesondere mit elektronischen Mitteln, sollte sichergestellt werden, dass:

- die betroffenen Personen ihre ausdrückliche Zustimmung gegeben haben (für B2C-Beziehungen);

- die Personen keinen Gebrauch von ihrem Recht auf Widerspruch gegen die Direktwerbung gemacht haben;
- die Nachrichten eine einfache Möglichkeit zur Abmeldung bieten („Opt-out");
- kein Empfänger die Namen und Kontaktdaten eines anderen Empfängers sehen kann.

J. Datenschutzverletzungen

Trotz der Anwendung hoher Standards zur Gewährleistung der Datensicherheit kann sich die Elior-Gruppe nicht vollständig gegen das Risiko von Datenverstößen schützen, die sich definieren können durch:

- Eine Verletzung der Vertraulichkeit, d.h. ein Datenverlust (z. B. Verlust eines USB-Sticks mit Kundendateien);
- eine Verletzung der Integrität, d.h. eine unvorhergesehene Änderung (z. B. eine unerwünschte Änderung der Datenbank, die den Behörden automatisch den Nutzungsberechtigten eines Firmenwagens anzeigt);
- ein Angriff auf die Verfügbarkeit, d.h. eine Zerstörung von Daten (z. B. Malware, die eine Datenbank verschlüsselt).

Die Quelle dieser Verletzungen kann extern (z.B. Angriff auf eine Ressource der Elior-Gruppe oder auf einen über das Internet verbundenen Dienstanbieter) oder intern sein. Sie kann absichtlich oder versehentlich sein (z. B. Bildschirm, der nicht durch einen in öffentlichen Verkehrsmitteln zu nutzenden Sichtschutz geschützt ist).

Jeder ist für Wachsamkeit verantwortlich und hat jede Datenschutzverletzung unverzüglich dem DSGVO-Team der Gruppe mitzuteilen. Im Falle einer nachgewiesenen oder vermuteten Verletzung der Sicherheit sollten unverzüglich Maßnahmen ergriffen werden, um die Auswirkungen und Schäden zu begrenzen. In schwerwiegenden Fällen muss die Elior-Gruppe die zuständige Datenschutzbehörde informieren und ihr innerhalb von 72 Stunden einen Aktionsplan zur Schadensbegrenzung vorlegen und in einigen Fällen auch die betroffenen Personen informieren.

K. Überwachung und Beziehung zu den Datenschutzbehörden

Mögliche Auswirkungen der Nichtbeachtung des Schutzes personenbezogener Daten

Verstöße gegen die Rechtsvorschriften zum Schutz personenbezogener Daten können schwerwiegende Folgen haben, insbesondere:

- Geldbußen von bis zu 4% des Gesamtumsatzes der Elior-Gruppe;
- Schadenersatzansprüche von Personen, die von der Verletzung der Privatsphäre betroffen sind;
- Erfüllung unter Geldbuße, Einschränkung der Verarbeitung oder die Aussetzung der Übermittlung von Daten;
- einen Ruf- und Imageschaden der Elior-Gruppe.

Befugnisse der Datenschutzbehörden

Die Elior-Gruppe arbeitet derzeit an *Binding Corporate Rules*. Zweck dieser BCR ist es, die Einhaltung eines gleichartigen Datenschutzniveaus, unabhängig vom Standort der Tochtergesellschaft der Elior-Gruppe, nachzuweisen und die Übermittlung personenbezogener Daten innerhalb der Elior-Gruppe zu genehmigen.

Die Behörde für den Schutz personenbezogener Daten ist befugt, die Einhaltung der Datenschutz-Grundverordnung durch Kontrollen vor Ort oder aus der Entfernung zu überwachen und kann insbesondere:

- Kopien so vieler technischer und rechtlicher Informationen wie möglich verlangen, um die Bedingungen für die Verarbeitung personenbezogener Daten zu beurteilen;
- die Übermittlung aller für die Erfüllung ihres Auftrags erforderlichen Dokumente verlangen;
- auf Computerprogramme und -daten zugreifen und deren Transkription anfordern;
- Kopien von Verträgen (z.B. Aktenmietverträge, Computerunterverträge), Formularen, Papierakten, Datenbanken, usw. anfordern,
- Remote-Scans auf Schwachstellen und Sicherheitsaudits durchführen und das Vorhandenseins von Rechtshinweisen überprüfen.

In Frankreich sieht Artikel 51 des geänderten Gesetzes Nr. 78-17 vom 6. Januar 1978 über die Datenverarbeitung, Dateien und Freiheitsrechte, bekannt als „Datenschutzgesetz", vor, dass jede Behinderung der Tätigkeit der CNIL mit einer Freiheitsstrafe von einem Jahr und einer Geldstrafe von 15.000 € geahndet werden kann. Eine Behinderung der Tätigkeit der Datenschutzbehörde liegt vor bei:

- Widerstand gegen die Erfüllung der Aufgaben, die den bevollmächtigten Mitgliedern oder Beauftragten übertragen wurden, wenn der Besuch vom Richter im Ermittlungs- und Strafverfahren genehmigt wurde;
- Weigerung, Informationen offenzulegen, Verschleierung oder Vernichtung von Informationen und Dokumenten, die für den Audit-Auftrag relevant sind;
- Übermittlung von Informationen, die nicht mehr dem Inhalt der Aufzeichnungen entsprechen, wie er zum Zeitpunkt der Anfrage der Datenschutzbehörde bestand, oder Inhalte in einer Form darzustellen, die nicht direkt zugänglich ist.

Erforderliche Maßnahmen:

Es wird empfohlen, sich umgehend mit dem Gruppenteam in Verbindung zu setzen und nach Überprüfung der Identität der Personen (Mandat und Berufsausweis) umfassend mit den Behörden zusammenzuarbeiten.

Das Gruppenteam ist die einzige Stelle, die berechtigt ist, mit den Datenschutzbehörden zu kommunizieren (z. B.: Vorabmaßnahme, Informationsanfrage, Beantwortung von Anrufungen usw.). Jedes Ersuchen der Behörden ist ihr daher unverzüglich mitzuteilen.

5. Zusätzliche Informationen

Wenn Sie Fragen zu dieser Richtlinie haben oder weitere Informationen zu einem der behandelten Themen wünschen, können Sie sich über die folgende E-Mail-Adresse an das Gruppenteam wenden: gdpr-contact@eliorgroup.com.