General Data Protection Regulation (GDPR) POLICY

Erstellt von:	Compliance
Erstellt am	07 Januar 2024
Genehmigt am:	25 Januar 2024
Genehmigt vom:	Geschäftsführerrat

Inhaltsverzeichnis

1. Ziel der GDPR Policy

Durch die stetige Entwicklung der Digitaltechnik erhält die Bedeutung des Datenschutzes immer mehr Aufmerksamkeit und stellt die SAMAG Europe Sarl („SAMAG“) regelmäßig vor große Herausforderungen, weil Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden.

Daher gilt der Grundsatz:
Wo Daten gespeichert und gesendet werden, muss ein hohes Maß an Datenschutz und Datensicherheit gewährleistet sein. Dies gilt für Daten von Kunden, Investoren, Interessenten und Geschäftspartnern genauso wie für Mitarbeiterdaten. Denn Datenschutz ist Schutz der Person.

Es ist der Anspruch der SAMAG einen hohen Standard beim Datenschutz zu setzen. Deshalb liegt es in der Pflicht des Unternehmens, den gesetzlichen Anforderungen zu entsprechen, die mit der Verarbeitung personenbezogener Daten verbunden sind. Es hat oberste Priorität, einen einheitlichen gültigen Standard für das Unternehmen beim Umgang mit personenbezogenen Daten sicherzustellen. Denn die Persönlichkeitsrechte und die Privatsphäre eines jeden Einzelnen zu wahren, ist die Basis für vertrauensvolle Geschäftsbeziehungen.

In dieser Policy sind die notwendigen Voraussetzungen für die Verarbeitung personenbezogener Daten von Kunden, Investoren, Investments, Interessenten, Geschäftspartnern und Mitarbeitern geregelt. Dadurch setzt die SAMAG einen gültigen Datenschutz- und Datensicherheitsstandard im Unternehmen und regelt den Datenaustausch intern sowie mit externen Partnern.

Ziel der GDPR Policy ist es, für den AIFM einheitliche, adäquate Datenschutzstandards aufzustellen, um die aus der Datenschutzgrundverordnung (DSGVO) folgende Anforderungen an den grenzüberschreitenden Datenverkehr zu genügen. Diese Richtlinie schafft in diesem Zusammenhang ein einheitliches Datenschutzniveau, ersetzt aber nicht die Legitimation, die jeder Verarbeitung oder Übermittlung zu Grunde legen muss. Daneben sollen die Mitarbeiter und Führungskräfte dabei unterstützt werden, Datenschutzbelange unserer Kunden, Investoren, Investments und Vertragspartner in die Gestaltung von Produkten und Dienstleistungen unseres Hauses zu integrieren.

2. Geltungsbereich

Diese Richtlinie ist eine Unternehmensrichtlinie und gilt sowohl für die Verarbeitung personenbezogener Daten von Mitarbeitern, Kunden und Investoren, Investments, als auch für die personenbezogenen Daten von Dritten, Beratern und anderen Vertragspartnern im gesamten Unternehmen.

Für die SAMAG ist die effektive Nutzung moderner Informations- und Kommunikationstechnologien ein wichtiger Bestandteil aller Geschäftsprozesse. Eine nicht sachgerechte oder missbräuchliche Verwendung dieser Technologie kann zur Verletzung von Persönlichkeitsrechten führen. Bei der Gestaltung der Informationsgesellschaft soll ein Ziel sein, den Schutz der Persönlichkeitsrechte in den Vordergrund zu stellen. Perfekte Betreuung und zuverlässige Auftragsabwicklung sind bedeutende Ziele der SAMAG und erfordern auch, auf Datenschutzbelange unserer Kunden, Investoren, Vertragspartner und Mitarbeiter einzugehen. Im Bewusstsein dieser Ziele verpflichtet sich das Unternehmen, die nachfolgenden Richtlinien einzuhalten.

3. Definitionen

- ***Betroffene*** im Sinne dieser Richtlinie sind alle Personen, mit denen eine Vertragsbeziehung besteht oder geplant ist, d.h. z. B. Kunden, Investoren, Investments und Mitarbeiter aber auch zukünftige Kunden, Investoren und Mitarbeiter in der Anbahnungsphase, allerdings nur, soweit personenbezogene Daten über diese Personen betroffen sind.
- ***Personenbezogene Daten*** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; 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.
- ***Verarbeitung*** personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.
- ***Befugte*** sind Mitarbeiter welche eine Erklärung zur Einhaltung der Datenschutzvorschriften unterzeichnen und entsprechend unterwiesen / sensibilisiert wurden.

Diese Mitarbeiter dürfen je nach Aufgabenstellung nur die für ihren Aufgabenbereich relevanten personenbezogenen Daten verarbeiten.

- ***Auftragsverarbeiter*** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- ***Dritter*** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
- ***Einwilligung*** der betroffenen Person ist 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. Die Einwilligung muss vor Beginn der Erhebung oder der Verarbeitung der Daten erfolgen. Eine rückwirkende Legitimation einer Verarbeitung kann durch eine Einwilligung nicht erfolgen.
- ***Profiling*** wird verstanden als jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Personen zu analysieren oder vorherzusagen.
- ***Privacy by Design*** beschreibt die bereits datenschutzfreundliche Entwicklung von Hard- und Software, was eine nachträgliche Anpassung und den damit verbundenen Mehraufwand vermeiden soll.
- ***Privacy by Default*** sieht eine datenschutzfreundliche Grundeinstellung von Hard- und Software vor, bei der die Nutzer im zweiten Schritt entscheiden können, ob und wie ihre Daten genutzt werden dürfen.
- Die ***Angemessenheit des Datenschutzniveaus*** wird in einem förmlichen Verfahren anerkannt. Die EU-Kommission hat die Möglichkeit, nach entsprechender Prüfung das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen. Die Feststellung kann auch auf ein bestimmtes Gebiet oder einen bestimmten Sektor in dem Drittland oder auch auf bestimmte Datenkategorien beschränkt sein. Ein angemessenes Schutzniveau besteht dann, wenn in dem Drittland auf Grundlage seiner innerstaatlichen Rechtsvorschriften und deren Anwendung, der Existenz und der wirksamen Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie seiner eingegangenen internationalen Verpflichtungen ein Schutzniveau existiert, welches dem in Luxemburg gewährten Schutzniveau gleichwertig ist.

4. Grundsätze für die Verarbeitung personenbezogener Daten

1. Bei der Datenverarbeitung müssen die Persönlichkeitsrechte der Betroffenen gewahrt werden.

2. Im Datenschutzrecht gilt das sogenannte Verbot mit Erlaubnisvorbehalt (Rechtmäßigkeit). Das heißt, die Datenverarbeitung ist generell verboten, so lange sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder der Betroffene in die Verarbeitung eingewilligt hat.
   Widerspricht ein Betroffener der Verarbeitung personenbezogener Daten, hat die Datenverarbeitung zu unterbleiben, sofern sie nicht trotz des Widerspruchs erlaubt ist.

3. Die Verarbeitung ist rechtmäßig, wenn sie auf einer entsprechenden Grundlage beruht (Rechtsgrundlage, Einwilligung etc.) und der Zweck der Verarbeitung von der Rechtsgrundlage bzw. der Einwilligung umfasst ist.

4. Die Daten dürfen nur für die genannten Zwecke verarbeitet werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck sachlich eng zusammenhängen.
   Unter bestimmten Voraussetzungen können personenbezogene Daten auch weiterverarbeitet werden, wenn die Verarbeitung nicht dem ursprünglichen Zweck entspricht. Hierfür muss der neue Zweck mit dem alten kompatibel sein, darf also für die betroffene Person nicht überraschend sein.
   Der Verantwortliche muss eine genaue, dokumentierte Prüfung anhand folgender festgelegter Kriterien durchführen:
   - Jede Verbindung zwischen den Zwecken,
   - Der Zusammenhang der Erhebung der Daten, insbesondere hinsichtlich des Verhältnisses zwischen der betroffenen Person und dem Verantwortlichen,
   - Die Art der personenbezogenen Daten (z. B. besonders sensible Daten),
   - Die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
   - Vorhandene Verschlüsselungen oder Pseudonymisierung der Daten.

   Ergibt die Prüfung, dass der Zweck nicht kompatibel ist, ist eine darauf gestützte Verarbeitung unzulässig, es sei denn, der Verantwortliche holt für den neuen Zweck wiederum eine Einwilligung ein.

5. Personenbezogene Daten müssen sachlich richtig und nach Möglichkeit aktuell gehalten werden. Es sind Maßnahmen dafür zu treffen, dass nichtzutreffende oder unvollständige Daten gelöscht bzw. berichtigt werden. Auch sind Maßnahmen zu treffen, dass Datensätze gesperrt werden können, um diese nach Ablauf von etwaigen Aufbewahrungsfristen löschen zu können.

6. Personenbezogene Daten dürfen nur in einer Form gespeichert werden, die die Identifizierung der Person solange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist. Sobald die

Speicherung personenbezogener Daten für den Verarbeitungszweck nicht mehr erforderlich ist, müssen die personenbezogenen Daten gelöscht oder die Identifizierung der betroffenen Person aufgehoben werden. Ausnahmen ergeben sich für im öffentlichen Interesse liegenden Archivzwecke, für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke.

7. Zugriff auf personenbezogene Daten dürfen nur Mitarbeiter haben, in deren Tätigkeitsbereich der Umgang mit diesen Daten fällt. Die Zugriffsberechtigung ist nach Art und Umfang des jeweiligen Tätigkeitsfeldes zu begrenzen.

   Die betroffene Person muss wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z. B. Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht etc.).

8. Die Datenverarbeitung hat sich an dem Ziel auszurichten, nur die erforderlichen personenbezogenen Daten, d. h. so wenig wie möglich, zu verarbeiten (Datenminimierung). Die Verarbeitung muss dabei in diesem Umfang verhältnismäßig (angemessen), zur Erreichung eines legitimen Zieles geeignet (erheblich) und nicht über das zur Zweckerreichung notwendige Maß hinausgehend sein. Die Instrumente der Anonymisierung und Pseudonymisierung sind zu nutzen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Statistische Auswertungen oder Untersuchungen, die auf der Basis anonymisierter oder pseudonymisierter Daten erfolgen, sind nicht datenschutzrelevant, soweit über diese Datensätze keine Rückschlüsse mehr auf die betroffenen Personen hergestellt werden können.

9. Zum Schutz der personenbezogenen Daten hat die SAMAG die Grundsätze des Datenschutzes durch Technik (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) zu berücksichtigen und geeignete interne Strategien festzulegen sowie entsprechende Maßnahmen zu setzen.
   Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

10. Entscheidungen, die für den Betroffenen eine rechtliche Wirkung nach sich ziehen oder ihn in ähnlicher Weise erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten (einschließlich Profiling) gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale wie z.B. der Kreditwürdigkeit dient. Die

Informationstechnik darf grundsätzlich nur als Hilfsmittel für eine Entscheidung herangezogen werden, ohne dabei deren einzige Grundlage zu bilden.
Das heißt, es sollte gewährleistet werden, dass in automatisierten Datensystemen keine personenbezogenen Daten weiterverarbeitet und verändert werden.
Sofern im Einzelfall die sachliche Notwendigkeit bestehen sollte, automatisierte Entscheidungen zu treffen, muss der Betroffene über eine automatisierte Verarbeitung und die Möglichkeit des Widerspruchs informiert werden. Der Verantwortliche muss angemessene und geeignete Maßnahmen treffen, um die Rechte, Freiheiten und berechtigten Interessen des Betroffenen zu wahren. Bei Datenverarbeitungsvorhaben, aus denen sich hohe Risiken für die Rechte und Freiheiten der Betroffenen ergeben können, ist der Bereich Datenschutz schon vor Beginn der Verarbeitung zu beteiligen und gegebenenfalls vorab eine Datenschutz-Folgenabschätzung vorzunehmen.

11. Das gesamte Unternehmen ist verantwortlich für den Datenschutz und seine Beachtung. Um die Einhaltung des Datenschutzes nachweisen zu können, muss eine entsprechende Dokumentation vorhanden sein.

5. Unterrichtung und Einwilligung der Betroffenen

1. Die vertragliche Beziehung

Personenbezogene Daten des Betroffenen dürfen auf der Grundlage bzw. zur Durchführung eines Vertrags-, bzw. Vertragsanbahnungsverhältnisses verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners nach Abschluss des Vertrages, sofern dies im Zusammenhang mit dem Vertragszweck steht.
Bereits bei der Erhebung ist der Betroffene darauf hinzuweisen, dass er über Auskunfts- und Berichtigungsrechte hinsichtlich seiner personenbezogenen Daten verfügt. Ferner sollte der Betroffene über die Freiwilligkeit der Angabe von Daten für Zwecke des Marketings unterrichtet werden.

Bei der Erhebung muss der Betroffene Folgendes erkennen können (Transparenz) und entsprechend informiert werden:

- Name und Kontaktdaten des Verantwortlichen, ggf. dessen Vertreters;
- Zweck der Datenverarbeitung samt Rechtsgrundlage für die Verarbeitung;
- Die verfolgten berechtigten Interessen, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erfolgt;
- Ggf. Dritte oder Kategorien von Dritten, an die die Daten übermittelt werden;
- Ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln;
- Dauer der Speicherung oder Kriterien für die Festlegung dieser Dauer;

- Das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- Wenn die Verarbeitung aufgrund einer Einwilligung des Betroffenen erfolgt, das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- Ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsschluss erforderlich ist, inwieweit der Betroffene verpflichtet ist, diese Daten bereitzustellen, und welche Folgen die Nichtbereitstellung hätte;
- Inwiefern eine automatisierte Entscheidungsfindung erfolgt (Profiling).

2. Beziehung ohne Vertragsverhältnis

Im Vorvertragsverhältnis ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Gleiches gilt für die Verarbeitung zur Erfüllung eines Vertrages mit der betroffenen Person. Sollten personenbezogene Daten erhoben werden, die über das zur Vertragsdurchführung oder -anbahnung Erforderliche hinausgehen, so ist eine Einwilligung des Betroffenen einzuholen.

Dasselbe gilt, wenn eine weitere Verarbeitung oder Nutzung von Daten außerhalb des ursprünglichen Erhebungszweckes erfolgen soll. Vor der Einwilligung muss der Betroffene unterrichtet werden.

Im Falle einer erforderlichen Einwilligungserklärung ist diese aus Beweisgründen regelmäßig schriftlich einzuholen und getrennt von sonstigen Regelungen optisch hervorzuheben.

In der Einwilligungserklärung müssen Umfang und Zweck der Datenverarbeitung spezifiziert werden. Im Falle besonderer Umstände, z. B. bei telefonischer Beratung, kann die Einwilligung ausnahmsweise auch mündlich erteilt werden. Für die Gestaltung von online abzugebenden Einwilligungserklärungen sind die Datenschutz- und Qualitätsstandards für e-Business zu beachten.

3. Datenerhebung bei einem Dritten/Datenaustausch

Grundsätzlich sind personenbezogene Daten beim Betroffenen selbst zu erheben. Sofern Daten bei Dritten erhoben bzw. von Dritten übermittelt werden, ist sicherzustellen, dass der Betroffene bei der ersten Ansprache entsprechend informiert ist oder wird, sofern nicht eine Ausnahme gem. Verordnung vorliegt.

Im Falle eines Datenerwerbs muss sichergestellt sein, dass die Daten im Rahmen des jeweils geltenden Rechts rechtmäßig erhoben wurden und rechtmäßig weitergegeben werden.

Eine Bonitätsprüfung bedarf keiner Einwilligung des Betroffenen, wenn ein überwiegendes berechtigtes Interesse besteht. Dieses liegt nur bei Kauf auf Rechnung vor.

Bei Zahlung per Lastschrift oder Vorkasse liegt kein überwiegendes berechtigtes Interesse vor und ist somit unzulässig. Weiterhin möglich ist eine Bonitätsprüfung jedoch, sofern der Betroffene hierin eingewilligt hat.

Generell werden alle anlegerbezogenen Daten über den Administrator AVEGA Fund Services S.à r.l. bearbeitet. Für solche Fälle verweisen wir auf die Datenschutzbestimmungen der AVEGA Fund Services S.à r.l..

Zur Erfüllung der zuvor genannten Zwecke übermittelt SAMAG Europe S.à r.l personenbezogene Daten an:

- Bestimmte Dienstleister, die Leistungen in unserem Auftrag erbringen,
- Bestimmte unabhängige Stellen, Finanzinstitute, Vertriebs- und Bankpartner mit denen SAMAG Europe S.à r.l regelmäßige Geschäftsbeziehungen unterhält.
- Aufsichtsbehörde, Finanzbehörden, Steuerbehörden
- Bestimmte Berufsgruppen wie Anwälte, Notare oder Wirtschaftsprüfer.

Für den Fall, dass SAMAG Daten über die Grenzen des Europäischen Wirtschaftsraum („EWR“) hinaus übermittelt, so erfolgt dies auf der Grundlage eines Beschlusses der Europäischen Kommission, in dem die Europäischen Kommission anerkannt hat, dass das Land, in das SAMAG Daten übermittelt, ein Datenschutzniveau bietet, das dem im EWR entspricht.
Es besteht derzeit kein ersichtlicher Grund mittel oder langfristig personenbezogenen Daten außerhalb des EWR zu übermitteln.

4. Datenaustausch innerhalb des Unternehmens

Einzelne Unternehmen einer Unternehmensgruppe sind zueinander grundsätzlich als Dritte anzusehen. Sofern ein Unternehmen personenbezogene Daten, für die es verantwortlich ist, gegenüber anderen Unternehmen, die derselben Unternehmensgruppe angehören, offenlegt, muss diese Offenlegung datenschutzrechtlich abgesichert werden:
Als verantwortliches Unternehmen kann die SAMAG andere Unternehmen innerhalb der Unternehmensgruppe als Auftragsverarbeiter einsetzen. Verantwortliche, die Teile einer Unternehmensgruppe sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke einschließlich der Verarbeitung personenbezogener Daten von Kunden, Investoren und Beschäftigten, zu übermitteln.
Hierzu muss ein Vertrag zur Auftragsverarbeitung mit jedem Unternehmen abgeschlossen werden.
Der Verantwortliche, der Teil einer Unternehmensgruppe ist, darf daher personenbezogene Daten innerhalb der Unternehmensgruppe übermitteln, sofern die empfangenden Unternehmen dieser Unternehmensgruppe ebenso angehören, die empfangenden Unternehmen dieser Unternehmensgruppe ihren Sitz innerhalb der EU/des EWR haben, es internen Verwaltungszwecken dient und im Falle einer gemeinsamen Verarbeitung eine Vereinbarung geschlossen wurde.

6. Art der genutzten Daten

Die SAMAG erhebt und nutzt solche personenbezogene Daten, die für die Aufrechterhaltung der Geschäftstätigkeit erforderlich sind. Die folgenden personenbezogenen Daten sieht SAMAG unter anderem vor zu erheben:

- Personenbezogene Identifikationsdaten, z.B. Name, Adresse(n), Telefonnummer(n)
- Von öffentlichen Stellen vergebene Legitimationsdaten, z.B. Personalausweis, Passnummer, Steuernummer, Sozialversicherungsnummer
- Angaben zur Person, z.B. Geburtsdatum, Geburtsort, Geschlecht, Personenstand, Staatsangehörigkeit
- Daten zur Zusammensetzung des Haushalts, z.B. Familienstand, Anzahl der Kinder, berufliche Tätigkeit
- Elektronische Kennung, z.B. E-Mail-Adresse, elektronische Signatur
- Bankdaten, z.B. Bankkontonummer, Einkommen,
- Angaben zu Schul -, Ausbildung - und Qualifikationsgrad, z.B. Bildungstand, Berufsqualifikationen,
- Angaben zu Beruf und Arbeitsverhältnis, z.B. Tätigkeiten, Name des Arbeitgebers, Gehalt,
- Daten aus Bildaufzeichnungen, z.B. Fotografien oder Digitalfotos,
- Geolokalisierungsdaten, z.B. bei der Einwahl in „FreeConferenceCall.com“.

Die von SAMAG verwendeten Daten zu Personen oder Firmen wurden von den jeweiligen Personen direkt zur Verfügung gestellt oder stammen aus folgenden Quellen um Datenbestände der SAMAG zu kompletieren:

- Aus Veröffentlichungen, die von öffentlichen Stellen bereitgestellt werden, z.B. Handelsregister
- Von Dienstleistern
- Von Internetseiten

7. Besondere Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person sind untersagt, sofern

sich die Rechtmäßigkeit der Verarbeitung nicht aus einer gesetzlichen Erlaubnis oder aus einem gesetzlichen Erfordernis ergibt.
Eine Verarbeitung besonderer Kategorien personenbezogener Daten ist ferner beispielsweise zulässig für die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche auch im Rahmen eines Rechtsstreits, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt oder der Betroffene in die Verarbeitung eingewilligt hat.

8. Rechte der Betroffenen

Betroffene können sich mit Fragen und Beschwerden direkt an den hierfür zuständigen Ansprechpartner im Unternehmen wenden. Insbesondere, wenn sie ihre nachfolgenden Rechte wahrnehmen, müssen diese Anfragen umgehend bearbeitet werden.

1. Recht auf Auskunft

Der Betroffene hat das Recht eine Bestätigung darüber zu verlangen, ob personenbezogene Daten seiner Person verarbeitet werden.
Wenn seine personenbezogenen Daten verarbeitet werden, kann Auskunft darüber verlangt werden, welche personenbezogenen Daten, aus welcher Herkunft und zu welchem Zweck gespeichert werden und welchen Empfängern die personenbezogenen Daten offengelegt werden. Wenn möglich, ist dem Betroffenen auch die geplante Dauer der Speicherung mitzuteilen. Falls dies nicht möglich ist, sind die Kriterien für die Festlegung der Speicherung mitzuteilen. Der Betroffene ist ferner über seine Rechte auf Berichtigung oder Löschung seiner personenbezogenen Daten und auf Einschränkung der Verarbeitung der Daten zu informieren.
Dem Betroffenen sind darüber hinaus sein Widerspruchsrecht und das Recht der Beschwerde bei einer Aufsichtsbehörde aufzuzeigen. Wenn eine automatisierte Entscheidungsfindung (Profiling) genutzt wird, ist der Betroffene über die involvierte Logik und Tragweite der angestrebten Auswirkungen zu informieren.

2. Recht auf Berichtigung

Sollte sich beispielsweise im Rahmen der Bearbeitung des Auskunftsrechts herausstellen, dass personenbezogene Daten unrichtig oder unvollständig sind, ist der Betroffene berechtigt, ohne unangemessene Verzögerung die Berichtigung bzw. Vervollständigung zu verlangen.

3. Recht auf Einschränkung der Verarbeitung

Eine betroffene Person kann vom Verantwortlichen unter folgenden Voraussetzungen die Einschränkung der Verarbeitung verlangen:

- Die Richtigkeit der Daten wird vom Betroffenen bestritten;

- Die Verarbeitung ist unrechtmäßig;
- Der Zweck der Verarbeitung hat sich erledigt, die Daten sind aber zur Geltendmachung von Rechtsansprüchen des Betroffenen notwendig;
- Es liegt ein Widerspruch des Betroffenen vor.

4. Recht auf Löschung

Die betroffene Person hat unter folgenden Voraussetzungen das Recht, die unverzügliche **Löschung** ihrer Daten zu verlangen („Recht auf Vergessenwerden“):

- Die Speicherung der Daten ist nicht mehr notwendig;
- Der Betroffene hat seine Einwilligung zur Datenverarbeitung widerrufen;
- Die Daten wurden unrechtmäßig verarbeitet;
- Es besteht eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht.

Das Recht auf Vergessenwerden findet unter folgenden Voraussetzungen keine Anwendung:

- Bei Überwiegen des Rechts auf freie Meinungsäußerung bzw. der Informationsfreiheit;
- Die Datenspeicherung dient der Erfüllung einer rechtlichen Verpflichtung (z. B. Aufbewahrungspflichten);
- Archivzwecke stehen der Löschung entgegen;
- Speicherung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht, muss die für die Verarbeitung der Daten verantwortliche Stelle unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen treffen und alle weiteren mit der Verarbeitung Beteiligten darüber informieren, dass eine betroffene Person die Löschung aller Links, Kopien oder Replikationen seiner personenbezogenen Daten verlangt hat. Die Berichtigung, Löschung oder Einschränkung der Verarbeitung muss dem Betroffenen mitgeteilt werden.

5. Recht auf Datenübertragbarkeit

Der Betroffene hat das Recht, die ihn betreffenden personenbezogenen Daten, welche dieser einem Verantwortlichen bereitgestellt hat, in einem gängigen Format zu erhalten und diese ohne Behinderung durch den Verantwortlichen an einen anderen Verantwortlichen weiterleiten zu lassen, sofern bspw. eine Einwilligung des Betroffenen vorliegt und die Verarbeitung mittels eines automatisierten Verfahrens erfolgt. Betroffene sollen dadurch leichter von einem Anbieter zu einem anderen wechseln können, ohne den Verlust ihrer Daten befürchten zu müssen.

6. Widerspruchsrecht

Der Betroffene kann gegen die Verarbeitung seiner personenbezogenen Daten Widerspruch erheben, der eine Weiterverarbeitung der Daten, abgesehen von einigen definierten Ausnahmen, für unzulässig erklärt. Zusätzlich hat er auch ein gesondertes ausdrückliches Widerspruchsrecht gegen die Verarbeitung von personenbezogenen Daten zum Zweck der Direktwerbung.

Soweit eine betroffene Person Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten erhebt, ist die Geschäftsführung zu informieren. Dies gilt nicht, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet oder die Verarbeitung der personenbezogenen Daten für die Durchführung des Vertrages notwendig ist.

7. Beschwerderecht

Betroffenen wird das Recht zuerkannt, sich bei der zuständigen Aufsichtsbehörde zu beschweren, wenn sie der Ansicht sind, dass eine Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder ein nationales Gesetz verstößt.

8. Folgen einer Verletzung von Rechten Betroffener

Zu beachten ist, dass dem Betroffenen bei rechtswidriger Verarbeitung seiner personenbezogenen Daten Unterlassungs- und Schadensersatzansprüche zustehen können.

Gemäß der geltenden Verordnung besteht das Recht, bei der zuständigen Kontrollbehörde Klage einzureichen:

Nationale Kommission für den Datenschutz / Commission nationale pour la protection des données - www.cnpd.lu.

Falls Fragen zur Verarbeitung personenbezogener Daten besteht, sollten diese schriftlich an die SAMAG Europe S.à r.l., 59, Esplanade de la Moselle, 6637 Wasserbillig, geschickt werden.

9. Vertraulichkeit der Verarbeitung

Nur Befugte und auf die Einhaltung des Datengeheimnisses sensibilisierte Mitarbeiter dürfen personenbezogene Daten verarbeiten. Insbesondere ist es untersagt, solche Daten für eigene private Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen. Unbefugt in diesem Sinne sind z. B. auch Arbeitskollegen, sofern sich nicht aufgrund des Tätigkeitsfeldes und der konkreten Aufgaben dieser Kollegen etwas anderes ergibt.
Diese Vertraulichkeit besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

10. Grundsätze der Datensicherheit

Das Unternehmen hat als verantwortliche Stelle sicherzustellen, dass personenbezogene Daten in einer Weise verarbeitet werden, die dem Stand der Technik entsprechen und ein angemessenes Schutzniveau aufweisen. Dies beinhaltet auch den Schutz gegen unberechtigte oder ungesetzliche

Verarbeitung. Darüber hinaus sind technische und organisatorische Maßnahmen zu treffen, die einen Verlust, die Zerstörung oder eine Schädigung von personenbezogenen Daten sowie die Beeinträchtigung von Persönlichkeits- und Freiheitsrechten verhindern sollen.
Um beurteilen zu können, was ein angemessenes Schutzniveau ist, muss im Vorfeld der Verarbeitung durch das Unternehmen geklärt werden, welchen Schutzbedarf die relevanten personenbezogenen Daten besitzen. Die Schutzbedarfsfeststellung ist als ein erster Schritt essentiell, wenn es später darum geht, geeignete und organisatorische Maßnahmen auszuwählen.
Im Datenschutzrecht sind vier Schutzziele aufgelistet, die bei der Verarbeitung personenbezogener Daten sicherzustellen sind.

Die Schutzziele sind:

1. Vertraulichkeit, d. h. Daten sind für Unberechtigte nicht zugänglich
2. Integrität, d. h. Daten können nicht verfälscht werden
3. Verfügbarkeit, d. h. Daten stehen zur Verfügung, wenn sie gebraucht werden
4. Belastbarkeit, d. h. die Widerstandsfähigkeit des Systems

Folgende Schritte sind zu beachten:

1. Schutzbedarf feststellen
2. Risiken bewerten / falls erforderlich Datenschutz-Folgenabschätzung durchführen
3. Maßnahmen treffen
4. Nachweise erbringen

Die zur Datensicherheit erforderlichen technisch-organisatorischen Maßnahmen beziehen sich auf:

- Rechner (Server und Arbeitsplatzrechner)
- Netze bzw. Kommunikationsverbindungen
- Applikationen

Hinsichtlich der Server sind physische und infrastrukturelle Sicherheitsmaßnahmen installiert, die Zutrittskontrollen (mit differenzierten Berechtigungen), Schließsysteme und Brandschutzmaßnahmen umfassen. Alle Arbeitsplatzrechner sind mit einem Passwortschutz ausgestattet. Das unternehmenseigene Netzwerk ist durch Firewall-Systeme vor unberechtigtem, externem Zugang und Zugriff aus dem Internet geschützt. Die Übertragung von Daten mit Personenbezug außerhalb des Netzwerks erfolgt verschlüsselt. Sofern hiervon abgewichen wird, ist dies dem Bereich Datenschutz gegenüber zu begründen. Zum Schutz der personenbezogenen Daten in den Datenbanken ist ein personen- und applikationsbezogener Zugangs- und Zugriffsschutz eingerichtet. Diese technisch-organisatorischen Maßnahmen sind in ein die Verantwortlichkeiten regelndes Datenschutz- und Sicherheitsmanagement einzubetten.

11. Telekommunikation und Internet

Die Verarbeitung personenbezogener Daten, die bei der Telekommunikation mit dem Betroffenen einschließlich der Internet-Kommunikation anfallen, richtet sich nach den vorhandenen Arbeitsanweisungen bzw. nach dem jeweils geltenden Recht.

12. Meldungen von Datenschutzverletzungen

Die Meldung einer Datenschutzverletzung an die Aufsichtsbehörde muss unverzüglich nachdem dem Verantwortlichen diese Verletzung bekannt wurde, erfolgen.

Die Meldung hat zumindest folgende Informationen zu enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (wenn möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der personenbezogenen Datensätze),
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Verantwortliche muss alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht.
Die betroffene Person ist im Falle eines voraussichtlich hohen Risikos unverzüglich von der Datenschutzverletzung zu benachrichtigen.

Diese Benachrichtigung muss zumindest Folgendes beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache,
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Eine Benachrichtigung der betroffenen Person ist nicht erforderlich, wenn

- auf die von der Verletzung betroffenen personenbezogenen Daten geeignete technische und organisatorische Sicherheitsvorkehrungen angewandt wurden (insbesondere, wenn dadurch unbefugte Personen keinen Zugang zu diesen Daten haben, etwa durch Verschlüsselung),
- der Verantwortliche durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht, oder
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall muss jedoch eine öffentliche Bekanntmachung erfolgen, oder eine ähnliche Maßnahme ergriffen werden, damit die betroffenen Personen vergleichbar wirksam informiert werden.

13. Verantwortlichkeiten und Berichterstattung

Die Geschäftsführung des Unternehmens ist verantwortlich für die Datenverarbeitung. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in dieser Richtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden. Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen.
Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter.
Bei Datenschutzkontrollen durch Behörden ist der Geschäftsführerrat umgehen zu informieren.
Die Geschäftsführung ist verpflichtet, umgehend Verletzungen der sich aus dieser Richtlinie ergebenden Verpflichtungen und Beschwerden an die Nationale Kommission für den Datenschutz (CNPD) zu melden.
Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen die Geschäftsführung rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren.
Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Geschäftsführerrat schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Führungskräfte müssen sicherstellen, dass alle Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden.
Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht können strafrechtlich verfolgt werden und Schadensersatzansprüche nach sich ziehen.

Eine interne Analyse, die durchgeführt wurde, um festzustellen, ob ein Datenschutzbeauftragter bestellt werden muss, hat aufgrund der unten aufgeführten Kriterien ergeben, dass die SAMAG keinen Datenschutzbeauftragten zu benennen hat:

Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln, - findet keine Anwendung

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, - findet keine Anwendung oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht - findet keine Anwendung

Es sind alle Mitarbeiter verpflichtet, im Falle einer Datenschutzverletzung innerhalb von SAMAG der Geschäftsführung und dem Compliance Officer den Vorfall zu melden.

14. Speicherung personenbezogener Daten

SAMAG speichert personenbezogene Daten für den Zeitraum, der zur Einhaltung der geltenden Rechtsbestimmungen erforderlich ist sowie zur Beantwortung von Justizanfragen oder Anfragen von staatlichen Stellen und Regulierungsbehörden festgelegt wurde. Dementsprechend werden die meisten personenbezogenen Daten unserer Investoren, Investments und Dienstleister während der gesamten Dauer der Vertragsbeziehung und für weitere 10 Jahre nach dem Ende der Vertragsbeziehung gespeichert.

15. Kontrolle der Dienstleister

Im Rahmen der regelmäßigen Due Diligence von Dienstleistern wird besprochen, ob der Dienstleister die personenbezogenen Daten entsprechend den Vorgaben der Verordnung angemessen verwaltet. Der Dienstleister muss über ausreichende Mechanismen verfügen, um eine ordnungsgemäße Führung, interne Kontrolle und Rechenschaftspflicht für die personenbezogenen Daten der Beteiligten zu gewährleisten.

Wenn dem Dienstleister eine Verletzung des Schutzes personenbezogener Daten in Bezug auf die vereinbarungsgemäß verarbeiteten personenbezogenen Daten bekannt wird, wird SAMAG unverzüglich informiert.