EXIDE TECHNOLOGIES
(„Exide“ oder „das Unternehmen“)

Datenschutzrichtlinie (die „Richtlinie“)

Es ist notwendig, dass Sie diese Richtlinie lesen, da sie wichtige Informationen zu folgenden Themen enthält:

- Die von Exide einzuhaltenden Datenschutzgrundsätze;
- Was personenbezogene Informationen (oder Daten) und sensible persönliche Informationen (oder Daten) sind;
- Wie Exide personenbezogene Daten und sensible personenbezogene Daten in Übereinstimmung mit den Richtlinien erfasst, verwendet und (letztendlich) löscht;
- Wo detailliertere Informationen zu den Daten zu finden sind, z. B. die personenbezogenen Daten, die Exide erhebt und verwendet, wie die personenbezogenen Daten verwendet, gespeichert und übertragen werden, zu welchen Zwecken, die Maßnahmen, die ergriffen werden, um diese personenbezogenen Daten sicher zu halten und wie lange sie aufbewahrt werden;
- Ihre Pflichten als Mitarbeiter von Exide in Bezug auf den Datenschutz; und
- Die Folgen der Nichteinhaltung dieser Richtlinie.

1 Einleitung

1.1 Exide erfasst, speichert und verwendet personenbezogene Daten (auch als „personenbezogene Daten“ bezeichnet) von Dritten für bestimmte rechtmäßige Zwecke, wie in den *Datenschutzhinweisen* von Exides dargelegt.

1.2 Diese Richtlinie legt fest, wie wir unseren Datenschutzverpflichtungen nachkommen. Der Zweck der Richtlinie besteht des Weiteren darin, sicherzustellen, dass Mitarbeiter, einschließlich Leih- und Zeitarbeitskräfte, die Regeln für die Erfassung, Verwendung und Löschung personenbezogener Daten, auf die sie während ihrer Arbeit möglicherweise Zugriff haben, verstehen und einhalten.

1.3 Exide verpflichtet sich zur Einhaltung unserer Datenschutzverpflichtungen und dazu, kurz, klar und transparent zu erläutern, wie wir personenbezogene Daten erhalten und verwenden und wie (und wann) wir diese Daten löschen, sobald sie nicht mehr benötigt werden.

1.4 Wenn Sie Fragen oder Kommentare zum Inhalt dieser Richtlinie haben oder weitere Informationen benötigen, wenden Sie sich an den lokalen Datenschutzbeauftragten oder an die Rechtsabteilung.

2 Anwendungsbereich

2.1 Die Mitarbeiter sollten sich auf die Datenschutzhinweise von Exide und gegebenenfalls auf die anderen relevanten Richtlinien von Exide beziehen, auch in Bezug auf die *Informationssicherheit und die Aufbewahrung von Unterlagen,* die weitere Informationen über den Schutz personenbezogener Daten in diesen Zusammenhängen enthalten.

2.2 Exide überprüft und aktualisiert diese Richtlinie in Übereinstimmung mit unseren Datenschutzverpflichtungen. Diese Richtlinie stellt keinen Bestandteil eines Arbeitsvertrags mit einem Mitarbeiter dar, und wir können die Richtlinie von Zeit zu Zeit ändern, aktualisieren oder ergänzen. Wir werden jede neue oder geänderte Richtlinie an die Mitarbeiter weiterleiten, wenn sie angenommen wird.

3 Definitionen

Strafregisterauszüge sind personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten,

Informationsbehauptungen, Verfahren und damit verbundene Sicherheitsmaßnahmen;

Datenschutzverletzung ist eine Sicherheitsverletzung, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, zur Änderung, zur unberechtigten Weitergabe oder zum unberechtigten Zugang zu personenbezogenen Daten führt;

Betroffene Person ist die Person, auf die sich die personenbezogenen Daten beziehen;

Personenbezogene (manchmal auch als personenbezogene Daten bezeichnet) sind Informationen über eine

betroffene Person, die (direkt oder indirekt) anhand dieser Daten identifiziert werden kann;

Verarbeitung bedeutet Beschaffung, Aufzeichnung, Organisation, Speicherung, Änderung, Abruf,

die Offenlegung und/oder Vernichtung von Daten oder, ganz allgemein, die Verwendung oder der Umgang mit ihnen;

Pseudonymisiert ist der Vorgang, bei dem personenbezogene Daten so verarbeitet werden, dass sie ohne die Verwendung zusätzlicher Informationen nicht zur Identifizierung einer betroffenen Person verwendet werden können, die getrennt aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die sicherstellen, dass die personenbezogenen Daten nicht einer identifizierbaren Person zugeordnet werden können;

Sensible personenbezogene Daten (manchmal auch als „besondere Kategorien personenbezogener Daten“ oder „sensible personenbezogene Daten“ bezeichnet) sind personenbezogene Informationen über die Rasse, die ethnische

Herkunft, die politischen Meinungen, die religiösen oder philosophischen Überzeugungen einer betroffenen Person, die Gewerkschaftszugehörigkeit (oder Nichtmitgliedschaft), genetische Informationen, biometrische Informationen (sofern sie zur Identifizierung einer betroffenen Person verwendet werden) und Informationen über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer betroffenen Person.

4 Datenschutzgrundsätze

4.1 Exide wird bei der Verarbeitung personenbezogener Daten die folgenden Datenschutzgrundsätze einhalten:

4.1.1 Wir werden personenbezogene Daten rechtmäßig, fair und transparent verarbeiten;

4.1.2 Wir erfassen personenbezogene Daten nur für festgelegte, ausdrückliche und rechtmäßige Zwecke und verarbeiten sie nicht auf eine Weise, die mit diesen rechtmäßigen Zwecken nicht vereinbar ist;

4.1.3 Wir verarbeiten nur die personenbezogenen Daten, die für die jeweiligen Zwecke angemessen, relevant und notwendig sind;

4.1.4 Wir werden genaue und aktuelle personenbezogene Daten aufbewahren und angemessene Schritte unternehmen, um sicherzustellen, dass ungenaue personenbezogene Daten unverzüglich gelöscht oder korrigiert werden;

4.1.5 Wir werden personenbezogene Daten in einer Form, die die Identifizierung der betroffenen Personen ermöglicht, nicht länger aufbewahren, als es für die Zwecke der Verarbeitung erforderlich ist; und

4.1.6 Wir werden geeignete technische und organisatorische Maßnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten sicher aufbewahrt und vor unbefugter oder rechtswidriger Verarbeitung sowie vor versehentlichem Verlust, Zerstörung oder Beschädigung geschützt werden.

5 Grundlage für die Verarbeitung personenbezogener Daten

5.1 In Bezug auf jede Verarbeitungsaktivität wird Exide, bevor die Verarbeitung zum ersten Mal beginnt, und dann regelmäßig, während sie fortgesetzt wird:

5.1.1 die Zwecke der jeweiligen Verarbeitung überprüfen und die geeignetste rechtmäßige Grundlage (oder Grundlagen) für diese Verarbeitung auswählen, d. h.:

(a) dass die betroffene Person der Verarbeitung zugestimmt hat;

(b) dass die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen, erforderlich ist;

(c) dass die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung, der das Unternehmen unterliegt, erforderliche ist;

(d) dass die Verarbeitung zum Schutz der wesentlichen Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist; oder

(e) dass die Verarbeitung für die berechtigten Interessen von Exide oder die des Unternehmens oder eines Dritten erforderlich ist, es sei denn, diese Interessen werden durch die Interessen der Grundrechte und -freiheiten der betroffenen Person außer Kraft gesetzt — siehe Ziffer 5.2 unten.

5.1.2 sofern die Verarbeitung nicht auf einer Einwilligung beruht, uns davon überzeugen, dass die Verarbeitung für den Zweck der entsprechenden Rechtsgrundlage erforderlich ist (d. h. dass es keine andere angemessene Möglichkeit gibt, diesen Zweck zu erreichen);

5.1.3 unsere Entscheidung, welche rechtliche Grundlage gilt, dokumentieren, um die Einhaltung der Datenschutzgrundsätze nachzuweisen;

5.1.4 Informationen sowohl über den Zweck der Verarbeitung als auch über die rechtmäßige Grundlage für die Verarbeitung in unsere(n) entsprechenden Datenschutzhinweis(e) aufnehmen;

5.1.5 dort, wo sensible personenbezogene Daten verarbeitet werden, auch eine rechtmäßige Sonderbedingung für die Verarbeitung dieser Daten ermitteln (siehe Abschnitt 6.2.2 unten) und diese dokumentieren (gilt nur für Vereinigtes Königreich); und

5.1.6 wenn Informationen über Straftaten im Einklang mit dem Recht der Union oder der Mitgliedstaaten verarbeitet werden, auch eine rechtmäßige Bedingung für die Verarbeitung dieser Informationen ermitteln und dokumentieren.

5.2 Wenn wir feststellen, ob die berechtigten Interessen des Unternehmens die geeignetste Grundlage für eine rechtmäßige Verarbeitung sind, werden wir:

5.2.1 eine angemessene Bewertung der berechtigten Interessen (legitimate interests assessment; LIA) durchführen und Aufzeichnungen darüber machen, um sicherzustellen, dass wir unsere Entscheidung rechtfertigen können;

5.2.2 wenn durch die LIA eine erhebliche Auswirkung auf die Privatsphäre erkannt wird, prüfen, ob wir auch eine Datenschutz-Folgenabschätzung (data protection impact assessment; DPIA) durchführen müssen; und

5.2.3 Informationen über unsere berechtigten Interessen in unsere(n) relevanten Datenschutzhinweis(e) aufnehmen.

6 Sensible personenbezogene Daten

6.1 Sensible personenbezogene Daten werden manchmal als „besondere Kategorien personenbezogener Daten“ bezeichnet.

6.2 Das Unternehmen muss möglicherweise von Zeit zu Zeit vertrauliche personenbezogene Daten verarbeiten. Wir verarbeiten vertrauliche personenbezogene Daten nur, wenn:

6.2.1 wir eine rechtliche Grundlage dafür, wie in Absatz 5.1.1 oben dargelegt, haben, z. B. ist es für die Erfüllung eines Arbeitsvertrags erforderlich, die gesetzlichen Verpflichtungen von Exide zu erfüllen oder dem berechtigten Interessen des Unternehmens nachzukommen; und

6.2.2 Es gilt eine der besonderen Bedingungen für die Verarbeitung sensibler personenbezogener Daten, z. B.:

(a) Die betroffene Person hat die Einwilligung erteilt;

(b) Die Verarbeitung ist zur Ausübung der arbeitsrechtlichen Rechte oder Pflichten von

Exide oder der betroffenen Person erforderlich;

(c) Die Verarbeitung ist erforderlich, um die wesentlichen Interessen der betroffenen Person zu schützen, und die betroffene Person ist physisch nicht in der Lage, eine Einwilligung zu erteilen;

(d) Die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offenkundig öffentlich gemacht hat, oder

(e) Die Verarbeitung ist zur Begründung, Geltendmachung oder Abwehr von Rechtsansprüchen erforderlich; oder

(f) Die Verarbeitung ist aus Gründen des erheblichen öffentlichen Interesses erforderlich.

6.3 Sensible personenbezogene Daten werden von Exide erst verarbeitet, wenn:

6.3.1 die betroffene Person ordnungsgemäß über die Art der Verarbeitung, die Zwecke, für die sie vorgenommen wird, und die Rechtsgrundlage dafür (mittels Datenschutzhinweis oder auf andere Weise) informiert wurde.

6.4 Das Unternehmen führt keine automatisierten Entscheidungen (einschließlich Profiling) auf der Grundlage der sensiblen personenbezogenen Daten einer betroffenen Person durch.

6.5 In der *Datenschutzerklärung* des Unternehmens sind die Arten von sensiblen personenbezogenen Daten aufgeführt, die Exide verarbeitet, wofür sie verwendet werden und die rechtmäßige Grundlage für die Verarbeitung.

6.6 In Bezug auf sensible personenbezogene Daten wird das Unternehmen die in den Absätzen 6.7 und 6.8 dargelegten Verfahren einhalten, um sicherzustellen, dass die in Absatz 4 dargelegten Datenschutzgrundsätze eingehalten werden.

6.7 **Während des Einstellungsverfahrens**: Die Personalabteilung von Exide wird sicherstellen (sofern das Gesetz nichts anderes zulässt), dass:

6.7.1 während der Phase der Vorauswahl, der Befragung und der Entscheidungsfindung keine Fragen zu sensiblen personenbezogenen Informationen gestellt werden, wie z. B. zur Rasse oder ethnischen Herkunft, Gewerkschaftsmitgliedschaft oder Gesundheit;

6.7.2 Das ausgefüllte Formular zur Überwachung der Chancengleichheit wird vom Antragsformular der betroffenen Person getrennt aufbewahrt und ist für die Person, die eine Auswahlliste erstellt, ein Vorstellungsgespräch führt oder eine Einstellungsentscheidung trifft, nicht einsehbar;

6.7.3 Überprüfungen des „Rechts auf Arbeit“ erfolgen, bevor ein Stellenangebot uneingeschränkt abgegeben wird, und nicht während der früheren Phasen der Vorauswahl, des Vorstellungsgespräches oder der Entscheidungsfindung;

6.8 **Während des Arbeitsverhältnisses**: Die Personalabteilung verarbeitet:

6.8.1 Gesundheitsinformationen für die Verwaltung des Krankengeldes, die Führung von Aufzeichnungen über krankheitsbedingte Fehlzeiten, die Überwachung der Anwesenheit des Personals und die Erleichterung der beschäftigungsbezogenen Gesundheits- und Krankenversicherungsleistungen;

6.8.2 sensible personenbezogene Daten zum Zwecke der Überwachung der Chancengleichheit. Soweit möglich, werden diese Informationen anonymisiert; und

6.8.3 Informationen über die Gewerkschaftsmitgliedschaft für die Zwecke der Personalverwaltung und der Verwaltung der Checkliste.

7 Strafregisterinformationen

Strafregisterinformationen werden in Übereinstimmung mit den Rechtsvorschriften der Union oder der Mitgliedstaaten verarbeitet.

8 Datenschutz-Folgenabschätzungen (DPIAs)

8.1 Besteht bei einer Datenverarbeitung ein hohes Risiko für die Datenschutzrechte einer

betroffenen Person (z. B. wenn Exide den Einsatz einer neuen Technologie plant), führen wir vor Beginn der Verarbeitung eine DPIA durch, um zu bewerten:

8.1.1 ob die Verarbeitung in Bezug auf ihren Zweck notwendig und verhältnismäßig ist;

8.1.2 ob Risiken für betroffene Personen bestehen; und

8.1.3 welche Maßnahmen ergriffen werden können, um diesen Risiken zu begegnen und personenbezogene Daten zu schützen.

8.2 Vor der Einführung einer neuen Technologie sollte sich der verantwortliche Manager daher mit der Abteilung Informationstechnologie in Verbindung setzen, damit eine DPIA durchgeführt werden kann.

8.3 Während einer DPIA wird das Unternehmen den Rat und die Ansichten anderer relevanter Interessenvertreter einholen.

9 Dokumentation und Aufzeichnung

9.1 Exide führt schriftliche Aufzeichnungen über die Verarbeitungsaktivitäten, einschließlich:

9.1.1 Name und Einzelheiten der Rechtspersönlichkeit von Exide (und gegebenenfalls anderer für die Verarbeitung Verantwortlicher);

9.1.2 die Zwecke der Verarbeitung;

9.1.3 eine Beschreibung der Kategorien der betroffenen Personen und der Kategorien personenbezogener Daten;

9.1.4 Kategorien von Empfängen der personenbezogenen Daten;

9.1.5 gegebenenfalls Einzelheiten zu Übermittlungen in Drittländer, einschließlich der Dokumentation der geltenden Schutzmaßnahmen für Übermittlungsmechanismen;

9.1.6 soweit möglich, Zeitpläne für die Aufbewahrung; und

9.1.7 soweit möglich eine Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen.

9.2 Im Rahmen unserer Aufzeichnung von Verarbeitungsaktivitäten dokumentieren wir oder verknüpfen mit der Dokumentation über:

9.2.1 Informationen, die für Datenschutzhinweise erforderlich sind;

9.2.2 Einverständniserklärungen;

9.2.3 Verträge des Verantwortlichen/Verarbeiters;

9.2.4 den Ort der personenbezogenen Daten;

9.2.5 DPIAs; und

9.2.6 Aufzeichnungen über Datenschutzverletzungen.

9.3 Wenn wir sensible personenbezogene Daten oder Strafregisterinformationen verarbeiten, führen wir schriftliche Aufzeichnungen über:

9.3.1 den (die) relevanten Zweck(e), für den (die) die Verarbeitung erfolgt, einschließlich (falls erforderlich) der Gründe, warum dies für diesen Zweck erforderlich ist;

9.3.2 die rechtmäßige Grundlage für unsere Verarbeitung; und

9.3.3 ob wir die personenbezogenen Daten gemäß unserem Richtliniendokument aufbewahren und löschen und, falls nicht, die Gründe für die Nichteinhaltung unserer Richtlinien.

9.4 Wir werden die von uns verarbeiteten personenbezogenen Daten regelmäßig überprüfen und unsere

Dokumentation entsprechend aktualisieren.

10 Rechte der betroffenen Personen

10.1 Die betroffenen Personen haben in Bezug auf ihre personenbezogenen Daten die folgenden Rechte:

10.1.1 darüber informiert zu werden, wie, warum und auf welcher Grundlage diese Daten verarbeitet werden — siehe *[Datenschutzhinweis]* von Exide;

10.1.2 eine Bestätigung zu erhalten, dass ihre Informationen verarbeitet werden, und Zugang zu ihnen und bestimmten anderen Informationen zu erhalten, indem sie einen Antrag auf Zugang stellen;

10.1.3 Daten korrigieren zu lassen, wenn sie fehlerhaft oder unvollständig sind;

10.1.4 Löschung von Daten, wenn sie für den Zweck, für den sie ursprünglich erfasst/verarbeitet wurden, nicht mehr erforderlich sind oder wenn kein zwingender berechtigter Grund für die Verarbeitung vorliegt (dies wird manchmal als „Recht auf Vergessen“ bezeichnet);

10.1.5 die Verarbeitung personenbezogener Daten einzuschränken, wenn die Richtigkeit der Daten beanstandet oder die Verarbeitung rechtswidrig ist; und

10.1.6 die Verarbeitung personenbezogener Daten vorübergehend einzuschränken, wenn sie ihrer Meinung nach nicht korrekt sind oder wenn sie der Verarbeitung widersprechen;

10.1.7 sofern gesetzlich vorgeschrieben, Richtlinien für die Speicherung, Löschung und Übermittlung ihrer personenbezogenen Daten nach Tod festzulegen.

11 Pflichten der betroffenen Personen

11.1 Einzelpersonen sind dafür verantwortlich, dass Exide ihre personenbezogenen Daten auf dem neuesten Stand hält. Möglicherweise haben Sie während Ihrer Beschäftigung oder Ihres Engagements Zugriff auf die personenbezogenen Daten anderer Mitarbeiter, Anbieter und Kunden. Wenn dies der Fall ist, erwartet das Unternehmen, dass Sie zur Erfüllung seiner Datenschutzverpflichtungen gegenüber den betroffenen Personen beitragen. Wenn Sie Zugang zu personenbezogenen Daten haben, dürfen/müssen Sie:

11.1.1 nur auf die persönlichen Daten zugreifen, für die Sie eine Zugangsberechtigung haben, und nur für autorisierte Zwecke;

11.1.2 anderen Mitarbeitern von Exide nur dann Zugang zu personenbezogenen Daten gewähren, wenn diese eine entsprechende Berechtigung haben;

11.1.3 Personen, die nicht Mitarbeiter des Unternehmens sind, nur dann den Zugang zu personenbezogenen Daten gestatten, wenn Sie von der Personal- oder Rechtsabteilung dazu ausdrücklich ermächtigt sind;

11.1.4 personenbezogene Daten sicher aufbewahren (z. B. durch die Einhaltung von Regeln für den Zugang zu Räumlichkeiten, den Zugang zu Computern, den Passwortschutz und die sichere Speicherung und Vernichtung von Dateien und andere Vorkehrungen, die in der globalen Informationssicherheitspolitik des Unternehmens festgelegt sind);

11.1.5 personenbezogene Daten oder Geräte, die personenbezogene Daten enthalten (oder die für den Zugang zu diesen Daten verwendet werden können), nicht aus den Räumlichkeiten des Unternehmens entfernen, es sei denn, es sind geeignete Sicherheitsmaßnahmen (wie Pseudonymisierung, Verschlüsselung oder Passwortschutz) vorhanden, um die Daten und das Gerät zu sichern; und

11.1.6 keine personenbezogene Daten auf lokalen Laufwerken oder auf persönlichen Geräten speichern, die für Arbeitszwecke verwendet werden.

11.2 Sie sollten sich an die Personalabteilung oder die Rechtsabteilung wenden, wenn Sie besorgt sind oder den Verdacht haben, dass Folgendes stattgefunden hat (oder stattfindet oder wahrscheinlich stattfinden wird):

11.2.1 Verarbeitung personenbezogener Daten ohne rechtmäßige Grundlage für deren Verarbeitung oder im Falle sensibler personenbezogener Daten;

11.2.2 jegliche Datenverletzung gemäß Absatz 15.1 unten;

11.2.3 Zugang zu personenbezogenen Daten ohne die entsprechende Genehmigung;

11.2.4 Personenbezogene Daten, die nicht sicher aufbewahrt oder gelöscht werden;

11.2.5 Entfernung von personenbezogenen Daten oder Geräten, die personenbezogene Daten enthalten (oder die für den Zugang zu diesen Daten verwendet werden können), aus den Räumlichkeiten des Unternehmens, ohne dass angemessene Sicherheitsmaßnahmen getroffen wurden;

11.2.6 jeder andere Verstoß gegen diese Richtlinie oder einen der in obigen Absatz 4.1 genannten Datenschutzgrundsätze.

12 Zugriff durch betroffene Personen

12.1 Eine betroffene Person kann jederzeit eine Anfrage („SAR“) stellen, um mehr über die personenbezogenen Daten zu erfahren, die das Unternehmen über sie aufbewahrt. Das Unternehmen ist in der Regel verpflichtet, die SAR innerhalb eines Monats nach Eingang zu beantworten (diese Frist kann bei komplexen und/oder zahlreichen Anträgen um bis zu zwei Monate verlängert werden, wobei die betroffene Person in diesen Fällen über die Notwendigkeit der Verlängerung informiert wird).

12.2 Alle eingehenden Anträge auf Zugang zum Thema müssen an den lokalen DSGVO-Korrespondenten weitergeleitet werden.

12.3 Das Unternehmen erhebt keine Gebühr für die Bearbeitung normaler SARs. Exide behält sich das Recht vor, angemessene Gebühren für zusätzliche Kopien von Daten zu erheben, die bereits an eine betroffene Person übermittelt wurden, oder für Anfragen, die offensichtlich unbegründet oder übertrieben sind, insbesondere wenn sich solche Anfragen wiederholen.

13 Informationssicherheit

13.1 Das Unternehmen wird geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit personenbezogener Daten zu gewährleisten und insbesondere vor unbefugter oder rechtswidriger Verarbeitung sowie vor versehentlichem Verlust, Zerstörung oder Beschädigung zu schützen. Das können unter anderem Folgende sein:

13.1.1 Sicherstellung, dass personenbezogene Daten nach Möglichkeit pseudonymisiert oder verschlüsselt werden;

13.1.2 Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und -dienste;

13.1.3 Sicherstellung, dass im Falle eines physischen oder technischen Zwischenfalls die Verfügbarkeit und der Zugang zu personenbezogenen Daten rechtzeitig wiederhergestellt werden können; und

13.1.4 Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit von technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

13.2 Wenn das Unternehmen externe Organisationen zur Verarbeitung personenbezogener Daten in seinem Namen einsetzt, müssen zusätzliche Sicherheitsvorkehrungen in Verträgen mit diesen Organisationen getroffen werden, um die Sicherheit personenbezogener Daten zu gewährleisten. Verträge mit externen Organisationen müssen insbesondere vorsehen, dass:

13.2.1 die Organisation nur nach schriftlichen Anweisungen von Exide handeln darf;

13.2.2 diejenigen, die die Daten verarbeiten, zur Vertraulichkeit verpflichtet sind;

13.2.3 geeignete Maßnahmen getroffen werden, um die Sicherheit der Verarbeitung zu gewährleisten;

13.2.4 Unterauftragnehmer nur mit vorheriger Zustimmung von Exide und unter einem schriftlichen Vertrag verpflichtet werden;

13.2.5 die Organisation Exide dabei unterstützen wird, Auskunft zu erteilen und den betroffenen Personen die Möglichkeit zu geben, ihre Rechte in Bezug auf den Datenschutz auszuüben;

13.2.6 die Organisation Exide bei der Erfüllung seiner Verpflichtungen in Bezug auf die Sicherheit der Verarbeitung, die Meldung von Datenschutzverletzungen und die Datenschutz-Folgenabschätzung unterstützen wird;

13.2.7 die Organisation alle personenbezogenen Daten löscht oder sie an Exide zurückgibt, wenn sie bei Vertragsende angefordert werden;

13.2.8 die Organisation sich Audits und Inspektionen unterzieht und Exide alle Informationen zur Verfügung stellt, die das Unternehmen benötigt, um sicherzustellen, dass Exide und die Organisation ihren Datenschutzverpflichtungen nachkommen; und

13.2.9 die Organisation Exide unverzüglich benachrichtigen wird, wenn sie gebeten wird, etwas zu unternehmen, das gegen das Datenschutzgesetz verstößt.

13.3 Bevor eine neue Vereinbarung über die Verarbeitung personenbezogener Daten durch eine externe Organisation geschlossen oder eine bestehende Vereinbarung geändert wird, müssen die betreffenden Mitarbeiter die Genehmigung der Bedingungen durch die Rechtsabteilung von Exide einholen.

14 Speicherung und Aufbewahrung personenbezogener Daten

14.1 Personenbezogene Daten (und sensible personenbezogene Daten) werden gemäß der globalen Informationssicherheitsrichtlinie des Unternehmens sicher aufbewahrt.

14.2 Personenbezogene Daten (und sensible personenbezogene Daten) sollten nicht länger als notwendig aufbewahrt werden. Wie lange die Daten aufbewahrt werden sollten, hängt von den Umständen ab, einschließlich der Gründe, aus denen die personenbezogenen Daten erhoben wurden. Die Mitarbeiter sollten die Richtlinie des Unternehmens zur Aufbewahrung von Unterlagen befolgen, in der die entsprechende Aufbewahrungsfrist bzw. die Kriterien, die zur Festlegung der Aufbewahrungsfrist herangezogen werden sollten, festgelegt sind. Bei Unklarheiten sollte sich das Personal an den örtlichen DSGVO-Korrespondenten oder an die Rechtsabteilung wenden.

15 Datenschutzverletzungen

15.1 Eine Datenschutzverletzung kann in vielerlei Hinsicht vorkommen, zum Beispiel:

15.1.1 Verlust oder Diebstahl von Daten oder Geräten, auf denen personenbezogene Daten gespeichert sind;

15.1.2 Unbefugter Zugriff auf oder unbefugte Verwendung von personenbezogenen Daten durch Mitarbeiter oder Dritte;

15.1.3 Datenverlust aufgrund eines Ausfalls von Geräten oder Systemen (einschließlich Hardware und Software);

15.1.4 Menschliches Versagen wie versehentliches Löschen oder Ändern von Daten;

15.1.5 Unvorhergesehene Umstände wie Brände oder Überschwemmungen;

15.1.6 Vorsätzliche Angriffe auf IT-Systeme wie Hacking, Viren oder Phishing; und

15.1.7 Erhalt von Informationen durch Täuschen der Organisation, die sie besitzt.

15.2 Das Unternehmen wird:

15.2.1 der zuständigen Aufsichtsbehörde oder dem Information Commissioner's Office (Vereinigtes Königreich) unverzüglich und nach Möglichkeit innerhalb von 72 Stunden nach Kenntnisnahme einer Datenschutzverletzung melden, wenn diese wahrscheinlich zu einer Gefährdung der Rechte und Freiheiten der betroffenen Personen führen wird; und

15.2.2 die betroffenen Personen benachrichtigen, wenn eine Datenschutzverletzung ein hohes Risiko für deren Rechte und Freiheiten darstellt und eine Benachrichtigung gesetzlich vorgeschrieben ist.

16 Internationale Datenübermittlung

16.1 Das Unternehmen kann personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums (EWR) (der die Länder der Europäischen Union sowie Island, Liechtenstein

und Norwegen umfasst) an die oberste Muttergesellschaft des Unternehmens, Exide Technologies in den Vereinigten Staaten von Amerika, auf der Grundlage übertragen, dass Exide Technologies als Unternehmen mit Standarddatenschutzklauseln bezeichnet wird.

17 Schulung

Das Unternehmen wird dafür sorgen, dass die Mitarbeiter in Bezug auf ihre Datenschutzverantwortung angemessen geschult werden. Personen, deren Rollen regelmäßigen Zugriff auf personenbezogene Daten erfordern oder die für die Umsetzung dieser Richtlinie oder die Beantwortung von Zugriffsanfragen im Rahmen dieser Richtlinie verantwortlich sind, erhalten zusätzliche Schulungen, die ihnen helfen, ihre Pflichten zu verstehen und diese einzuhalten.

18 Folgen bei Nichteinhaltung

18.1 Das Unternehmen nimmt die Einhaltung dieser Richtlinie sehr ernst. Die Nichteinhaltung der Richtlinie:

18.1.1 gefährdet die betroffenen Personen, deren personenbezogene Daten verarbeitet werden; und

18.1.2 birgt das Risiko erheblicher zivil- und strafrechtlicher Sanktionen für den Einzelnen und das Unternehmen; und

18.1.3 kann unter Umständen eine Straftat des Einzelnen darstellen.

18.2 Aufgrund der Bedeutung dieser Richtlinie kann die Nichteinhaltung von Anforderungen durch einen Mitarbeiter zu Disziplinarmaßnahmen im Rahmen unserer Verfahren führen, und diese Maßnahmen können zur Entlassung wegen groben Fehlverhaltens führen. Verstößt jemand, der kein Mitarbeiter ist, gegen diese Richtlinie, kann sein Vertrag mit sofortiger Wirkung gekündigt werden.

18.3 Wenn Sie Fragen oder Bedenken zu dieser Richtlinie haben, zögern Sie nicht, sich an den DSGVO-Landesvertreter oder die Rechtsabteilung zu wenden.