

EXIDE TECHNOLOGIES ("Exide" of "de Onderneming")

Beleid inzake gegevensbescherming (het "Beleid")

U bent verplicht dit beleid te lezen omdat het belangrijke informatie biedt over:

- de beginselen inzake gegevensbescherming waaraan Exide moet voldoen;
- wat zijn persoonsgegevens (of gegevens) en gevoelige persoonsgegevens (of gegevens);
- hoe Exide persoonsgegevens en gevoelige persoonsgegevens verzamelt, gebruikt en (uiteindelijk) verwijdert in overeenstemming met het Beleid;
- waar meer gedetailleerde informatie over de gegevens kan worden gevonden, bijvoorbeeld de persoonsgegevens die Exide verzamelt en gebruikt, hoe de persoonsgegevens worden gebruikt, opgeslagen en overgedragen, voor welke doeleinden, welke maatregelen zijn genomen om die persoonlijke gegevens te beveiligen en voor hoe lang deze worden bewaard;
- uw verplichtingen als Exide-medewerker met betrekking tot gegevensbescherming; en
- de gevolgen van het niet-naleven van dit Beleid.

1 Inleiding

- 1.1 Exide verkrijgt, bewaart en gebruikt persoonlijke gegevens (ook wel "persoonsgegevens" genoemd) over derden voor een aantal specifieke wettige doeleinden, zoals uiteengezet in Exide zijn *privacy kennisgeving inzake gegevensbescherming*.
- 1.2 Dit Beleid zet uiteen hoe wij ons houden aan onze verplichtingen inzake gegevensbescherming. Het doel van het Beleid is ook ervoor te zorgen dat personeel, inclusief werknemers, en uitzendkrachten de regels voor het verzamelen, gebruiken en verwijderen van persoonsgegevens waar zij tijdens hun werkzaamheden toegang tot hebben, begrijpen en naleven.
- 1.3 Exide verplicht zich om te voldoen aan onze verplichtingen inzake gegevensbescherming en om beknopt, duidelijk en transparant te zijn over hoe wij persoonsgegevens verkrijgen, gebruiken en hoe (en wanneer) wij die gegevens verwijderen als deze niet langer nodig zijn.
- 1.4 Als u vragen of opmerkingen heeft over de inhoud van dit Beleid of als u meer informatie nodig hebt, dient u contact op te nemen met de plaatselijke AVG-correspondent of de juridische afdeling.

2 Toepassingsgebied

- 2.1 Medewerkers dienen de *privacy kennisgeving inzake gegevensbescherming* van Exide en (waar van toepassing zijnde) andere relevante beleidsregels te raadplegen, waaronder met betrekking tot de *gegevensbeveiliging en het bewaren van documenten*, die verdere informatie over de bescherming van persoonsgegevens in die context bevatten.
- 2.2 Exide zal dit Beleid in overeenstemming met onze verplichtingen inzake gegevensbescherming herzien en bijwerken. Dit Beleid maakt geen deel uit van enig arbeidsovereenkomst van een werknemer en we kunnen het Beleid van tijd tot tijd wijzigen, bijwerken of aanvullen. Wij zullen ieder nieuw of aangepast beleid onder het personeel verspreiden wanneer het wordt goedgekeurd.

3 Definities

strafregistergegevens	zijn persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten, beschuldigingen, procedures en bijbehorende veiligheidsmaatregelen;
datalek	betekent een inbreuk op de beveiliging die leidt tot de toevallige of onwettige vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van of toegang tot persoonsgegevens;
betrokkene	de persoon op wie de persoonsgegevens betrekking hebben;
persoonsgegevens	(ook bekend als persoonlijke gegevens) zijn gegevens gerelateerd aan een betrokkene die direct of indirect kan worden geïdentificeerd uit die gegevens;
informatieverwerking	betekent het verkrijgen, opnemen, organiseren, opslaan, wijzigen, ophalen, bekendmaken en/of vernietigen van gegevens, of meer in het algemeen het gebruiken of er iets mee doen;
Gepseudonimiseerd	betekent het proces waarbij persoonsgegevens zodanig worden verwerkt dat deze niet kunnen worden gebruikt om een betrokkene te identificeren zonder gebruik te maken van aanvullende gegevens, die afzonderlijk worden bewaard en die zijn onderworpen aan technische en organisatorische maatregelen om ervoor te zorgen dat de persoonsgegevens niet kunnen worden toegeschreven aan een identificeerbare betrokkene;
gevoelige persoonsgegevens	(ook wel 'speciale categorieën van persoonsgegevens' of 'gevoelige persoonsgegevens' genoemd) zijn persoonsgegevens over biometrische informatie (waar gebruikt om een betrokkene te identificeren) en gegevens over de gezondheid van een betrokkene.

4 beginselen inzake gegevensbescherming

- 4.1 Exide voldoet bij het verwerken van persoonsgegevens aan de volgende beginselen inzake gegevensbescherming:
- 4.1.1 wij verwerken persoonsgegevens op een rechtmatige, eerlijke en transparante wijze;
 - 4.1.2 wij zullen persoonsgegevens alleen voor specifieke, expliciete en legitieme doeleinden verzamelen en zullen deze niet verwerken op een manier die onverenigbaar is met die legitieme doeleinden;
 - 4.1.3 wij zullen alleen de persoonsgegevens verwerken die adequaat, relevant en noodzakelijk zijn voor de relevante doeleinden;
 - 4.1.4 wij houden persoonsgegevens volledig en actueel bij en nemen redelijke maatregelen om ervoor te zorgen dat onjuiste persoonsgegevens onverwijld worden verwijderd of gecorrigeerd;
 - 4.1.5 wij zullen persoonsgegevens in een vorm die identificatie van betrokkenen mogelijk maakt, niet langer dan noodzakelijk bewaren voor de doeleinden waarvoor de gegevens worden verwerkt; en
 - 4.1.6 wij zullen passende technische en organisatorische maatregelen nemen om ervoor te zorgen dat persoonsgegevens veilig worden bewaard en beschermd tegen ongeoorloofde of onwettige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

5 Grondslag voor het verwerken van persoonsgegevens

- 5.1 In verband met enige verwerkingsactiviteit zal Exide, voordat de verwerking voor de eerste keer begint, en vervolgens regelmatig, terwijl het doorgaat:

- 5.1.1 de doeleinden van de specifieke verwerkingsactiviteit beoordelen en de meest geschikte wettelijke grondslag (of grondslagen) voor die verwerking selecteren, dat wil zeggen:
- (a) dat de betrokkene heeft ingestemd met de verwerking;
 - (b) dat de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is of om stappen te ondernemen op verzoek van de betrokkene voorafgaand aan het sluiten van een overeenkomst;
 - (c) dat de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting waaraan de Onderneming is onderworpen;
 - (d) dat de verwerking noodzakelijk is voor de bescherming van de vitale belangen van de betrokkene of een andere natuurlijke persoon; of
 - (e) dat de verwerking noodzakelijk is voor de legitieme belangen van Exide of die van de Onderneming of een derde partij, behalve wanneer die belangen worden geschonden door de belangen van fundamentele rechten en vrijheden van de betrokkene - zie artikel 5.2 hieronder.
- 5.1.2 behalve wanneer de verwerking op toestemming is gebaseerd om ons ervan te overtuigen dat de verwerking noodzakelijk is voor het doel van de relevante wettelijke grondslag (dat wil zeggen dat er geen andere redelijke manier is om dat doel te bereiken);
- 5.1.3 onze beslissing documenteren over welke wettelijke grondslag van toepassing is, om ons te helpen aantonen dat we voldoen aan de beginselen inzake gegevensbescherming;
- 5.1.4 informatie bijvoegen over zowel de doeleinden van de verwerking als de wettelijke grondslag daarvoor in onze relevante privacyverklaring(en);
- 5.1.5 waar gevoelige persoonsgegevens worden verwerkt, ook een wettelijke speciale voorwaarde voor het verwerken van die gegevens identificeren (zie paragraaf 6.2.2 hieronder) en deze documenteren (alleen voor het Verenigd Koninkrijk); en
- 5.1.6 waar gegevens betreffende strafrechtelijke overtredingen in overeenstemming met de wetgeving van de Unie of de lidstaten worden verwerkt, moet ook een wettelijke voorwaarde voor de verwerking van die gegevens worden vastgesteld en worden gedocumenteerd.
- 5.2 Bij het bepalen of de legitieme belangen van de Onderneming de meest geschikte basis voor rechtmatige verwerking zijn, zullen wij:
- 5.2.1 een gepaste beoordeling van de legitieme belangen (LIA) uitvoeren en deze vastleggen, om ervoor te zorgen dat we onze beslissing kunnen rechtvaardigen;
 - 5.2.2 indien de LIA een aanzienlijk effect op de privacy vaststelt, moet worden bekeken of wij ook een effectbeoordeling voor gegevensbescherming (DPIA) moeten uitvoeren; en
 - 5.2.3 informatie over onze legitieme belangen opnemen in onze relevante privacyverklaring(en).

6 Gevoelige persoonsgegevens

- 6.1 Gevoelige persoonsgegevens worden soms 'speciale categorieën van persoonlijke gegevens' of 'gevoelige persoonlijke gegevens' genoemd.
- 6.2 De Onderneming kan van tijd tot tijd gevoelige persoonsgegevens verwerken. Wij zullen alleen gevoelige persoonsgegevens verwerken indien:
- 6.2.1 wij hiervoor een wettelijke grondslag hebben, zoals uiteengezet in paragraaf 5.1.1 hierboven, het bijvoorbeeld noodzakelijk is voor de uitvoering van een arbeidsovereenkomst om te voldoen aan de wettelijke verplichtingen van Exide of aan de legitieme belangen van de Onderneming; en
 - 6.2.2 een van de speciale voorwaarden voor het verwerken van gevoelige persoonlijke gegevens van toepassing is, bijvoorbeeld:

- (a) de betrokkene heeft uitdrukkelijke toestemming gegeven;
- (b) de verwerking is noodzakelijk voor de uitoefening van de arbeidsrechten of -verplichtingen van Exide of de betrokkene;
- (c) de verwerking is noodzakelijk om de vitale belangen van de betrokkene te beschermen en de betrokkene kan niet fysiek instemmen;
- (d) de verwerking heeft betrekking op persoonsgegevens die door de betrokkene klaarblijkelijk openbaar zijn gemaakt;
- (e) de verwerking is noodzakelijk voor het instellen, uitoefenen of verdedigen van rechtsovereenkomsten; of
- (f) de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang.

6.3 Gevoelige persoonsgegevens worden door Exide niet verwerkt totdat:

6.3.1 de betrokkene op de juiste wijze is geïnformeerd (via een privacyverklaring of anderszins) over de aard van de verwerking, de doeleinden waarvoor deze wordt uitgevoerd en de rechtsgrondslag daarvoor.

6.4 De Onderneming voert geen geautomatiseerde besluitvorming (inclusief profilering) uit op basis van de gevoelige persoonsgegevens van een betrokkene.

6.5 De *privacy kennisgeving inzake gegevensbescherming* van de Onderneming geeft de soorten gevoelige persoonsgegevens weer die Exide verwerkt, waarvoor ze worden gebruikt en de wettelijke grondslag voor de verwerking.

6.6 Met betrekking tot gevoelige persoonsgegevens zal de Onderneming voldoen aan de procedures uiteengezet in de paragrafen 6.7 en 6.8 hieronder om ervoor te zorgen dat er wordt voldaan aan de beginselen inzake gegevensbescherming zoals uiteengezet in paragraaf 4 hierboven.

6.7 **Tijdens het rekruteringsproces:** de afdeling personeelszaken van Exide zorgt ervoor dat (behalve waar de wet anderszins toestaat):

6.7.1 tijdens de voorselectie, het interview en de besluitvormingsfase er geen vragen gesteld worden met betrekking tot gevoelige persoonsgegevens, zoals bijv. ras of etnische afkomst, vakbondslidmaatschap of gezondheid;

6.7.2 een volledig ingevuld monitoringformulier voor gelijke kansen gescheiden wordt gehouden van het aanvraagformulier van de betrokkene en wordt niet gezien door de persoon die de voorselectie doet, een interview afneemt of de aanwervingsbeslissing neemt;

6.7.3 "recht op werk"-controles worden uitgevoerd voordat een aanbod tot dienstverband onvoorwaardelijk wordt gedaan, en niet tijdens de eerdere voorselectie, het interview of de besluitvormingsfasen;

6.8 **Gedurende dienstverband:** verwerkt de afdeling personeelszaken:

6.8.1 gezondheidsgegevens met het oog op het beheer van het ziekengeld, het bijhouden van ziekteverzuimregisters, toezicht houden op de aanwezigheid van het personeel en het faciliteren van arbeid gerelateerde gezondheidsvoordelen en ziekte-uitkeringen;

6.8.2 gevoelige persoonsgegevens met het oog op het monitoren van gelijke kansen. Waar mogelijk worden deze gegevens geanonimiseerd; en

6.8.3 gegevens betreffende vakbondslidmaatschap ten behoeve van personeelsadministratie en beheer van 'afrekenen'.

7 **Strafregistergegevens**

Strafregistergegevens worden verwerkt in overeenstemming met de wetgeving van de Unie of de lidstaten.

8 Effectbeoordelingen van gegevensbescherming (DPIA's)

- 8.1 Wanneer de verwerking waarschijnlijk resulteert in een hoog risico voor de rechten inzake gegevensbescherming van een betrokkene (bijvoorbeeld wanneer Exide van plan is een nieuwe vorm van technologie te gebruiken), voeren wij, alvorens met de verwerking te beginnen, een DPIA uit om te beoordelen:
- 8.1.1 of de verwerking noodzakelijk en evenredig is in verhouding tot het doel;
 - 8.1.2 de risico's voor betrokkenen; en
 - 8.1.3 welke maatregelen kunnen worden getroffen om die risico's aan te pakken en persoonsgegevens te beschermen.
- 8.2 Voordat een nieuwe vorm van technologie wordt geïntroduceerd, dient de verantwoordelijke manager daarom contact op te nemen met de afdeling Informatietechnologie zodat een DPIA kan worden uitgevoerd.
- 8.3 Tijdens een DPIA zal de Onderneming advies en standpunten van andere relevante belanghebbenden inwinnen.

9 Documentatie en records

- 9.1 Exide houdt schriftelijke records bij van verwerkingsactiviteiten, waaronder:
- 9.1.1 de naam en gegevens van de Exide-rechtspersoon (en indien van toepassing, van andere beheerders);
 - 9.1.2 de doeleinden van de verwerking;
 - 9.1.3 een beschrijving van de categorieën van betrokkenen en categorieën van persoonsgegevens;
 - 9.1.4 categorieën van ontvangers van persoonsgegevens;
 - 9.1.5 indien van toepassing, bijzonderheden over overdrachten aan derde landen, met inbegrip van documentatie over de bestaande beschermingsmechanismen van de overdracht;
 - 9.1.6 waar mogelijk bewaartermijnen; en
 - 9.1.7 waar mogelijk een beschrijving van technische en organisatorische beveiligingsmaatregelen.
- 9.2 Als onderdeel van onze registratie van verwerkingsactiviteiten documenteren wij, of maken een link naar documentatie, over:
- 9.2.1 gegevens vereist voor privacy verklaringen;
 - 9.2.2 records van toestemming;
 - 9.2.3 overeenkomsten verwerkingsverantwoordelijke en verwerker;
 - 9.2.4 de locatie van persoonsgegevens;
 - 9.2.5 DPIA's; en
 - 9.2.6 gegevens van datalekken.
- 9.3 Als wij gevoelige persoonsgegevens of strafregistergegevens verwerken, houden wij schriftelijke records bij van:
- 9.3.1 het (de) relevante doel(en) waarvoor de verwerking plaatsvindt, inclusief (waar nodig) waarom dit voor dat doel noodzakelijk is;
 - 9.3.2 de wettelijke grondslag voor onze verwerking; en
 - 9.3.3 of we de persoonsgegevens behouden en wissen in overeenstemming met ons beleidsdocument en, zo niet, de redenen om ons beleid niet te volgen.
- 9.4 We zullen regelmatig de door ons verwerkte persoonsgegevens beoordelen en onze documentatie dienovereenkomstig bijwerken.

10 Rechten van betrokkenen

- 10.1 Betrokkenen hebben de volgende rechten met betrekking tot hun persoonsgegevens:
- 10.1.1 om te worden geïnformeerd over hoe, waarom en op welke basis die gegevens worden verwerkt—zie de [*privacy kennisgeving van Exide*];
 - 10.1.2 om bevestiging te verkrijgen dat hun gegevens worden verwerkt en om toegang te krijgen tot deze gegevens en bepaalde andere gegevens, door een verzoek als betrokkene om toegang te doen;
 - 10.1.3 om gegevens te laten corrigeren als deze onjuist of onvolledig zijn;
 - 10.1.4 om gegevens te laten wissen als deze niet langer nodig zijn voor het doel waarvoor ze oorspronkelijk zijn verzameld/verwerkt, of als er geen doorslaggevende legitieme redenen zijn voor de verwerking (dit wordt soms ook wel "het recht om te worden vergeten" genoemd);
 - 10.1.5 om de verwerking van persoonsgegevens te beperken wanneer de juistheid van de gegevens wordt betwist, of de verwerking onwettig is; en
 - 10.1.6 om de verwerking van persoonsgegevens tijdelijk te beperken wanneer zij denken dat deze niet juist zijn, of wanneer zij bezwaar hebben gemaakt tegen de verwerking;
 - 10.1.7 om richtlijnen vast te stellen, waar wettelijk verplicht, het bewaren, wissen en communiceren van hun persoonsgegevens na overlijden.

11 Verplichtingen van betrokkenen

- 11.1 Individuen zijn verantwoordelijk om Exide te helpen hun persoonsgegevens actueel te houden. Mogelijk hebt u tijdens uw dienstverband of samenwerking toegang tot de persoonsgegevens van andere werknemers, leveranciers en klanten. Als dat het geval is, verwacht de Onderneming dat u helpt zijn verplichtingen inzake gegevensbescherming met betrekking tot die betrokkenen na te komen. Als u toegang hebt tot persoonsgegevens, bent u verplicht om:
- 11.1.1 alleen de persoonsgegevens te openen waartoe u toegang hebt verkregen en alleen voor geautoriseerde doeleinden;
 - 11.1.2 alleen ander personeel van Exide toegang te verlenen tot persoonsgegevens als deze over de juiste autorisatie beschikt;
 - 11.1.3 alleen toegang tot persoonsgegevens te verlenen aan personen die geen personeel van het bedrijf zijn als u daarvoor specifieke toestemming hebt van de afdeling personeelszaken of juridische afdelingen;
 - 11.1.4 persoonsgegevens veilig te houden (bijvoorbeeld door te voldoen aan regels over toegang tot gebouwen, computertoegang, wachtwoordbeveiliging en beveiligde bestandsopslag en vernietiging en andere voorzorgsmaatregelen die uiteengezet zijn in het wereldwijde gegevensbeveiligingsbeleid van de Onderneming);
 - 11.1.5 geen persoonsgegevens, of apparaten die persoonsgegevens bevatten (of die kunnen worden gebruikt om er toegang toe te hebben), uit de gebouwen van de Onderneming te verwijderen, tenzij passende veiligheidsmaatregelen zijn getroffen (zoals pseudonimisering, codering of wachtwoordbeveiliging) om de informatie en het apparaat te beveiligen; en
 - 11.1.6 geen persoonsgegevens op te slaan op lokale stations of op persoonlijke apparaten die voor werkdoeleinden worden gebruikt.
- 11.2 U dient contact op te nemen met de afdeling personeelszaken of de juridische afdeling als u zich zorgen maakt of vermoedt dat een van de volgende zaken heeft plaatsgevonden (of plaatsvindt of waarschijnlijk zal plaatsvinden):
- 11.2.1 verwerking van persoonsgegevens zonder wettelijke grondslag voor de verwerking ervan of, in het geval van gevoelige persoonsgegevens;

- 11.2.2 een datalek zoals uiteengezet in paragraaf 15.1 hieronder;
- 11.2.3 toegang tot persoonsgegevens zonder de juiste toestemming;
- 11.2.4 niet veilig bewaarde of verwijderde persoonsgegevens;
- 11.2.5 verwijdering van persoonsgegevens, of apparaten die persoonsgegevens bevatten (of die kunnen worden gebruikt om toegang te krijgen tot deze gegevens), van de gebouwen van de Onderneming zonder dat passende beveiligingsmaatregelen zijn getroffen;
- 11.2.6 enige andere schending van dit beleid of van een van de beginselen inzake gegevensbescherming uiteengezet in paragraaf 4.1 hierboven.

12 Toegang van betrokkene

- 12.1 Een betrokkene kan op elk moment een verzoek ("SAR") indienen om meer te weten te komen over de persoonsgegevens die de Onderneming over hen bewaart. De Onderneming dient normaliter binnen één maand na ontvangst op SAR's reageren (dit kan met maximaal twee maanden worden verlengd in geval van complexe en/of talrijke verzoeken, en in dergelijke gevallen zal de betrokkene worden geïnformeerd over de noodzaak van de verlenging).
- 12.2 Alle ontvangen toegangsverzoeken van betrokkenen moeten worden doorgestuurd naar de lokale AVG-correspondent.
- 12.3 De Onderneming rekent geen vergoeding voor het verwerken van normale SAR's. Exide behoudt zich het recht voor om redelijke vergoedingen in rekening te brengen voor extra exemplaren van gegevens die reeds aan een betrokkene zijn verstrekt, of voor verzoeken die kennelijk ongegrond of buitensporig zijn, met name wanneer dergelijke verzoeken herhaaldelijk voorkomen.

13 Informatie beveiliging

- 13.1 De Onderneming zal passende technische en organisatorische maatregelen nemen om persoonsgegevens te beveiligen, en in het bijzonder om te beschermen tegen ongeoorloofde of onwettige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Deze kunnen omvatten:
 - 13.1.1 ervoor zorgen dat, waar mogelijk, persoonsgegevens wordt gepseudonimiseerd of gecodeerd;
 - 13.1.2 zorgen voor de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten;
 - 13.1.3 ervoor zorgen dat, in geval van een fysiek of technisch incident, de beschikbaarheid en toegang tot persoonsgegevens tijdig kan worden hersteld; en
 - 13.1.4 een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen om de beveiliging van de verwerking te waarborgen.
- 13.2 Wanneer het bedrijf externe organisaties gebruikt om namens hem persoonsgegevens te verwerken, dienen aanvullende beveiligingsregelingen te worden geïmplementeerd in overeenkomsten met deze organisaties om de beveiliging van persoonsgegevens te waarborgen. In het bijzonder moeten overeenkomsten met externe organisaties bepalen dat:
 - 13.2.1 de organisatie alleen mag handelen volgens de schriftelijke instructies van Exide;
 - 13.2.2 degenen die de gegevens verwerken zijn onderworpen aan een geheimhoudingsplicht;
 - 13.2.3 passende maatregelen worden genomen om de beveiliging van de verwerking te waarborgen;
 - 13.2.4 onderaannemers alleen worden ingeschakeld met voorafgaande toestemming van Exide en op basis van een schriftelijke overeenkomst;

- 13.2.5 de organisatie zal Exide helpen bij het bieden van toegang aan de betrokkenen en het mogelijk maken dat betrokkenen hun rechten met betrekking tot gegevensbescherming kunnen uitoefenen;
 - 13.2.6 de organisatie zal Exide assisteren bij het nakomen van zijn verplichtingen met betrekking tot de beveiliging van de verwerking, de melding van datalekken en effectbeoordelingen over gegevensbescherming;
 - 13.2.7 de organisatie zal alle persoonsgegevens verwijderen of retourneren aan Exide zoals vereist bij de afloop van de overeenkomst;
 - 13.2.8 de organisatie zal zich onderwerpen aan audits en inspecties, Exide voorzien van alle gegevens die de Onderneming nodig heeft om ervoor te zorgen dat zowel Exide als de organisatie aan hun verplichtingen inzake gegevensbescherming voldoen; en
 - 13.2.9 de organisatie zal Exide onmiddellijk op de hoogte stellen indien zij wordt gevraagd om iets te doen dat inbreuk maakt op de wet inzake gegevensbescherming.
- 13.3 Voordat een nieuwe overeenkomst waarbij persoonsgegevens door een externe organisatie worden verwerkt, wordt gesloten of een bestaande overeenkomst wordt gewijzigd, moet het desbetreffende personeel goedkeuring vragen voor de voorwaarden bij de juridische afdeling van Exide.

14 Opslag en bewaren van persoonsgegevens

- 14.1 Persoonsgegevens (en gevoelige persoonsgegevens) zullen veilig worden bewaard in overeenstemming met het wereldwijde informatiebeveiligingsbeleid van de Onderneming.
- 14.2 Persoonsgegevens (en gevoelige persoonsgegevens) mogen niet langer worden bewaard dan nodig is. Hoelang de gegevens dienen te worden bewaard, is afhankelijk van de omstandigheden, inclusief de redenen waarom de persoonsgegevens werden verkregen. Medewerkers dienen het beleid voor het bewaren van gegevens van de Onderneming te volgen, waarin de relevante bewaartermijn uiteen is gezet, of de criteria die gebruikt dient te worden om de bewaartermijn te bepalen. Als er enige onzekerheid is, dient het personeel de plaatselijke AVG-correspondent of de juridische afdeling te raadplegen.

15 Datalekken

- 15.1 Een datalek kan vele verschillende vormen aannemen, zoals bijvoorbeeld:
 - 15.1.1 verlies of diefstal van gegevens of apparatuur waarop persoonsgegevens zijn opgeslagen;
 - 15.1.2 ongeoorloofde toegang tot of gebruik van persoonsgegevens door een personeelslid of een derde;
 - 15.1.3 verlies van gegevens als gevolg van een defect aan apparatuur of systemen (inclusief hardware en software);
 - 15.1.4 menselijke fouten, zoals per ongeluk verwijderen of wijzigen van gegevens;
 - 15.1.5 onvoorziene omstandigheden, zoals een brand of overstroming;
 - 15.1.6 opzettelijke aanvallen op IT-systemen, zoals hacking, virussen of phishing; en
 - 15.1.7 waar gegevens worden verkregen door de organisatie die deze beheert te misleiden.
- 15.2 De Onderneming zal:
 - 15.2.1 het vereiste rapport van een datalek onverwijld en indien mogelijk binnen 72 uur zodra men op de hoogte is, melden aan de bevoegde autoriteit of informatiecommissaris (Verenigd Koninkrijk), indien dit mogelijk een risico voor de rechten en vrijheden van betrokkenen oplevert; en
 - 15.2.2 de getroffen betrokkenen op de hoogte brengen als een datalek mogelijk resulteert in een hoog risico voor hun rechten en vrijheden en kennisgeving wettelijk verplicht is.

16 Internationale overdrachten

- 16.1 De Onderneming kan persoonsgegevens buiten de Europese Economische Ruimte (EER) (die de landen van de Europese Unie en IJsland, Liechtenstein en Noorwegen omvat)

overdragen naar de uiteindelijke moedermaatschappij van de Onderneming, Exide Technologies in de Verenigde Staten van Amerika, op voorwaarde dat Exide Technologies wordt aangeduid als houder van standaardbepalingen voor gegevensbescherming.

17 Training

De Onderneming zorgt ervoor dat het personeel voldoende is opgeleid met betrekking tot hun verantwoordelijkheden op het gebied van gegevensbescherming. Personen wiens functies regelmatige toegang tot persoonsgegevens vereisen of die verantwoordelijk zijn voor de uitvoering van dit beleid of die reageren op verzoeken van betrokkenen om toegang onder dit beleid, zullen een aanvullende training krijgen om hen te helpen hun plichten te begrijpen en hoe eraan te voldoen.

18 Gevolgen van niet-naleving

18.1 De Onderneming neemt dit beleid zeer serieus. Niet-naleving van dit beleid:

18.1.1 brengt de betrokkenen waarvan de persoonsgegevens worden verwerkt in gevaar; en

18.1.2 brengt het risico op aanzienlijke civiele en strafrechtelijke sancties voor het individu en de Onderneming met zich mee; en

18.1.3 kan in sommige omstandigheden leiden tot een strafrechtelijke overtreding van het individu.

18.2 Vanwege het belang van dit beleid kan het niet-naleven door een medewerker van enige vereiste leiden tot disciplinaire maatregelen volgens onze procedures, en deze actie kan leiden tot ontslag wegens grove fouten. Als een niet-werknemer dit beleid schendt, kan zijn/haar overeenkomst met onmiddellijke ingang worden beëindigd.

18.3 Indien u vragen of opmerkingen heeft over iets in dit beleid, aarzel dan niet om contact op te nemen met de landelijke vertegenwoordiger van de AVG of de juridische afdeling.