26 juni 2018

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

Beleid inzake gegevensbescherming (het "Beleid")

Er wordt van u verlangd dat u dit beleid leest omdat het belangrijke informatie bevat over:

- de beginselen van gegevensbescherming waar Exide aan moet voldoen;
- wat persoonlijke informatie (of gegevens) is en gevoelige persoonlijke informatie (of gegevens);
- hoe Exide persoonlijke informatie en gevoelige persoonlijke informatie in overeenstemming met dit beleid verzamelt, gebruikt en (tenslotte) verwijdert;
- wanneer meer gedetailleerde informatie met betrekking tot de gegevens kan worden gevonden, bijvoorbeeld de persoonlijke informatie die Exide verzamelt en gebruikt, hoe de persoonlijke informatie wordt gebruikt, opgeslagen en overgedragen, voor welke doeleinden de stappen die worden genomen om deze persoonlijke informatie vertrouwelijk te houden en voor hoe lang dit wordt bewaard;
- uw verplichtingen als werknemer van Exide met betrekking tot gegevensbescherming; en
- de gevolgen van het niet naleven van dit beleid.

1 Introductie

1.1 Exide verkrijgt, bewaart en gebruikt persoonlijke informatie (ook "persoonsgegevens" genoemd) over derden voor een aantal specifieke wettelijke doeleinden, zoals uiteengezet in Exide's *kennisgevingen inzake gegevensbescherming.*

1.2 In dit beleid wordt uiteengezet hoe wij voldoen aan onze verplichtingen inzake gegevensbescherming. Het doel van dit beleid is ook om ervoor te zorgen dat het personeel, waaronder werknemers, tijdelijke werknemers en uitzendkrachten de voorschriften voor het verzamelen, het gebruik en het verwijderen van persoonlijke informatie die zij tijdens hun werk kunnen inzien, begrijpen en naleven.

1.3 Exide verbindt zich ertoe haar verplichtingen inzake gegevensbescherming na te komen en zakelijk, duidelijk en transparant te zijn over hoe wij persoonlijke informatie verkrijgen en gebruiken en hoe (en wanneer) de informatie wordt verwijderd zodra deze niet langer nodig is.

1.4 Als u vragen of opmerkingen hebt over de content van dit beleid of wanneer u meer informatie wilt hebben, kunt u contact opnemen met de lokale AVG-correspondent of de juridische afdeling.

2 Scoop

2.1 Werknemers dienen te verwijzen naar Exide's kennisgevingen inzake gegevensbescherming en, indien van toepassing, naar haar andere relevante beleidslijnen onder meer met betrekking tot de *informatiebeveiliging en het bewaren van documenten,* die verdere informatie bevatten met betrekking tot het beschermen van persoonlijke informatie in deze context.

2.2 Exide herziet en actualiseert dit beleid in overeenstemming met haar verplichtingen inzake gegevensbescherming. Dit beleid maakt geen deel uit van enige arbeidsovereenkomst en we kunnen het beleid van tijd tot tijd wijzigen, bijwerken of aanvullen. We verspreiden elk nieuw of gewijzigd beleid onder het personeel zodra dit van toepassing is.

3 Definities

strafregisters betekent persoonlijke informatie met betrekking tot strafrechtelijke veroordelingen en overtredingen,

informatie beschuldigingen, procedures, en gerelateerde veiligheidsmaatregelen;

gegevensinbreuk betekent een inbreuk op de beveiliging die leidt tot het accidenteel of onwettig vernietigen, verlies, wijzigen, ongeoorloofd bekendmaken van, of toegang tot persoonlijke informatie;

gegevenssubject betekent de persoon op wie de persoonlijke informatie betrekking heeft;

persoonlijke gegevens (soms ook wel persoonsgegevens genoemd) betekent informatie met betrekking tot een gegeven

informatie persoon die (direct of indirect) aan de hand van de informatie kan worden geïdentificeerd;

verwerking betekent het verkrijgen, opnemen, organiseren, opslaan, wijzigen, ophalen,

informatie openbaren en/of het vernietigen van informatie, of meer in het algemeen gebruiken of er van alles mee doen;

Pseudonimisering betekent het proces waarbij persoonlijke informatie zodanig wordt verwerkt dat het niet kan worden gebruikt voor het identificeren van een gegevenssubject zonder het gebruik van aanvullende informatie, die afzonderlijk wordt bewaard en is onderworpen aan technische en organisatorische maatregelen om ervoor te zorgen dat de persoonlijke informatie niet kan worden toegeschreven aan een identificeerbaar gegevenssubject;

Gevoelige persoonlijke informatie (soms bekend als 'speciale categorieën van persoonsgegevens' of 'gevoelige persoonsgegevens') betekent persoonlijke informatie over het ras, de etnische oorsprong, politieke opvattingen, religieuze of filosofische overtuigingen, vakbondslidmaatschap (of niet-lidmaatschap), genetische informatie, biometrische gegevens (voor zover die worden gebruikt voor het identificeren van een gegevenssubject) en informatie met betrekking tot de gezondheid, het seksleven of de seksuele oriëntatie van een gegevenssubject.

4 Beginselen van gegevensbescherming

4.1 Exide zal bij het verwerken van persoonlijke informatie voldoen aan de volgende beginselen van gegevensbescherming:

4.1.1 we verwerken persoonlijke informatie rechtmatig, eerlijk en op een transparante wijze;

4.1.2 we verzamelen persoonlijke informatie uitsluitend voor specifieke, expliciete en legitieme doeleinden en we verwerken deze niet op een manier die onverenigbaar is met die legitieme doeleinden;

4.1.3 we verwerken uitsluitend persoonlijke informatie die adequaat, relevant en nodig is voor de desbetreffende doeleinden;

4.1.4 we houden de persoonlijke informatie nauwkeurig bij en up-to-date en nemen redelijke stappen om ervoor te zorgen dat onnauwkeurige persoonlijke informatie zonder vertraging wordt verwijderd of gecorrigeerd;

4.1.5 we houden persoonlijke informatie bij in een vorm die de identificatie van gegevenssubjecten mogelijk maakt en voor een periode die niet langer is dan noodzakelijk voor de doeleinden waarvoor de informatie wordt verwerkt; en

4.1.6 we nemen de passende technische en organisatorische maatregelen om ervoor te zorgen dat de persoonlijke informatie veilig wordt bewaard, beschermd tegen ongeoorloofde of onwettige verwerking en tegen accidenteel verlies, vernietiging of schade.

5 Basis voor het verwerken van persoonlijke informatie

5.1 Met betrekking tot alle verwerkingsactiviteiten zal Exide, voordat er wordt begonnen met de verwerking, en vervolgens op regelmatige basis:

5.1.1 de doeleinden van de desbetreffende verwerkingsactiviteiten evalueren en de meest geschikte wettelijke basis (of bases) voor die verwerking selecteren, d.w.z.:

(a) dat het gegevenssubject akkoord is gegaan met de verwerking;

(b) dat de verwerking noodzakelijk is voor de uitvoering van een overeenkomst waar het gegevenssubject deel van uitmaakt of om op verzoek van het gegevenssubject stappen te ondernemen alvorens een overeenkomst te sluiten;

(c) dat de verwerking noodzakelijk is voor de naleving van een wettelijke verplichting waartoe de vennootschap verplicht is;

(d) dat de verwerking noodzakelijk is voor de bescherming van de vitale belangen van het gegevenssubject of een andere natuurlijke persoon; of

(e) dat de verwerking noodzakelijk is voor Exide's legitieme belangen of die van de vennootschap of een externe partij, behalve waar die belangen worden tenietgedaan door de belangen van de fundamentele rechten en vrijheden van het gegevenssubject—zie clausule 5.2 hieronder.

5.1.2 behalve wanneer de verwerking is gebaseerd op toestemming, onszelf ervan te verzekeren dat de verwerking noodzakelijk is voor het doel van de desbetreffende wettelijke basis (d.w.z. dat er geen andere verantwoorde manier is om dat doel te bereiken);

5.1.3 onze beslissing over welke wettelijke basis van toepassing is te documenteren om te helpen aantonen dat wij voldoen aan de beginselen van gegevensbescherming;

5.1.4 informatie over zowel de doeleinden van de verwerking en de wettelijke basis ervoor in onze desbetreffende privacyverklaring(en) op te nemen;

5.1.5 wanneer gevoelige persoonlijke informatie wordt verwerkt ook een wettelijke bijzondere voorwaarde vaststellen voor het verwerken van die informatie (zie paragraaf 6.2.2 hieronder), en dit te documenteren (uitsluitend voor het VK); en

5.1.6 wanneer informatie met betrekking tot een misdrijf wordt verwerkt in overeenstemming met het recht van de Unie of van een lidstaat ook een rechtmatige voorwaarde voor de verwerking van die informatie te identificeren en te documenteren.

5.2 Bij het bepalen of de legitieme belangen van de vennootschap de meest geschikte basis zijn voor de rechtmatige verwerking, zullen wij:

5.2.1 een passende beoordeling van de legitieme belangen (LIA) uitvoeren en hiervan een dossier bijhouden om ervoor te zorgen dat wij onze beslissing kunnen verantwoorden;

5.2.2 in het geval dat de LIA een aanzienlijke impact op de privacy identificeert, overwegen of wij ook een privacyeffectbeoordeling (DPIA) moeten uitvoeren; en

5.2.3 informatie met betrekking tot onze legitieme belangen opnemen in onze desbetreffende privacyverklaring(en).

6 Gevoelige persoonlijke informatie

6.1 Gevoelige persoonlijke informatie wordt soms aangeduid als 'speciale categorieën van persoonsgegevens' of 'gevoelige persoonlijke gegevens'.

6.2 De vennootschap moet van tijd tot tijd gevoelige persoonlijke informatie verwerken. Wij verwerken uitsluitend gevoelige persoonlijke informatie als:

6.2.1 we hiervoor een rechtmatige basis hebben zoals uiteengezet in paragraaf 5.1.1 hierboven, d.w.z. dat dit noodzakelijk is voor het uitvoeren van een arbeidsovereenkomst, om te voldoen aan Exide's wettelijke verplichtingen of voor de legitieme belangen van de vennootschap; en

6.2.2 als één van de bijzondere voorwaarden voor het verwerken van gevoelige persoonlijke informatie van toepassing is, bijvoorbeeld:

(a) als het gegevenssubject geen expliciete toestemming heeft;

(b) als de verwerking noodzakelijk is voor het uitoefenen van de arbeidsrechtelijke rechten of plichten van Exide of het gegevenssubject;

(c) als de verwerking noodzakelijk is voor het beschermen van de vitale belangen van het gegevenssubject en het gegevenssubject fysiek niet in staat is om toestemming te geven;

(d) als de verwerking betrekking heeft op persoonsgegevens die duidelijk door het gegevenssubject openbaar zijn gemaakt;

(e) als de verwerking noodzakelijk is voor het vaststellen, uitoefenen of verdedigen van rechtsvorderingen; of

(f) als de verwerking noodzakelijk is om reden van zwaarwegend openbaar belang.

6.3 Gevoelige persoonlijke informatie wordt niet door Exide verwerkt totdat:

6.3.1 het gegevenssubject naar behoren is geïnformeerd (door middel van een privacyverklaring of anderszins) over de aard van de verwerking, de doeleinden waarvoor dit wordt uitgevoerd en de rechtsgrond ervan.

6.4 De vennootschap voert geen geautomatiseerde besluitvorming (waaronder profilering) uit op basis van alle gevoelige persoonlijke informatie van het gegevenssubject.

6.5 De *kennisgevingen inzake gegevensbescherming* van de vennootschap beschrijven de soorten van gevoelige persoonlijke informatie die door Exide worden verwerkt, waar deze voor wordt gebruikt en de wettelijke basis voor de verwerking.

6.6 Met betrekking tot gevoelige persoonlijke informatie zal de vennootschap de procedures naleven die in de paragrafen 6.7 en 6.8 hieronder worden uiteengezet om ervoor te zorgen dat het voldoet aan de beginselen van gegevensbescherming zoals uiteengezet in paragraaf 4 hierboven.

6.7 **Tijdens het wervingsproces**: De afdeling Human Resources van Exide zorgt ervoor dat (behalve wanneer de wet anderszins voorschrijft):

6.7.1 tijdens de fasen van selectie, interview en besluitvorming er geen vragen worden gesteld met betrekking tot gevoelige persoonlijke informatie, bijvoorbeeld ras of etnische oorsprong, vakbondslidmaatschap of de gezondheid;

6.7.2 elk ingevuld verslag inzake het toezicht op gelijke kansen afzonderlijk van het sollicitatieformulier van het gegevenssubject wordt bewaard en niet zichtbaar is voor de persoon die de selectie, het interview of het aanwervingsbesluit uitvoert;

6.7.3 'recht op werk'-controles worden uitgevoerd voordat een functie definitief wordt aangeboden en niet tijdens de fasen van selectie, interview of besluitvorming;

6.8 **Tijdens het dienstverband**: de afdeling Human Resources verwerkt:

6.8.1 gezondheidsinformatie ten behoeve van het beheer van ziekte-uitkeringen, het bijhouden van een register van ziekteverzuim, het toezicht op personeelsopkomst en het faciliteren van aan arbeid gerelateerde gezondheidszorg en ziekte-uitkeringen;

6.8.2 gevoelige persoonlijke informatie voor het toezicht op gelijke kansen. Waar mogelijk wordt deze informatie geanonimiseerd; en

6.8.3 informatie over vakbondslidmaatschap ten behoeve van de personeelsadministratie en het beheer van de 'check off'.

7 Informatie uit het strafregister

Informatie uit het strafregister wordt verwerkt in overeenstemming met de wetgeving van de Unie of een lidstaat.

8 Privacyeffectbeoordelingen (DPIA's)

8.1 Indien de verwerking naar alle waarschijnlijkheid leidt tot een groot risico voor de rechten van het gegevenssubject op het gebied van gegevensbescherming (bijvoorbeeld wanneer Exide van plan is een nieuwe vorm van technologie te ontwikkelen), zullen wij voordat de verwerking begint, een DPIA uitvoeren om te beoordelen:

8.1.1 of de verwerking noodzakelijk is en in verhouding staat tot het doel;

8.1.2 de risico's voor gegevenssubjecten; en

8.1.3 welke maatregelen kunnen worden genomen om die risico's te identificeren en persoonlijke informatie te beschermen.

8.2 Voordat een nieuwe vorm van technologie wordt geïntroduceerd, dient de verantwoordelijke manager daarover contact op te nemen met de IT-afdeling, zodat een DPIA kan worden uitgevoerd.

8.3 Tijdens een DPIA zal de vennootschap advies en de standpunten van alle andere relevante belanghebbenden inwinnen.

9 Documenten en gegevens

9.1 Exide houdt een schriftelijk dossier bij van verwerkingsactiviteiten, waaronder:

9.1.1 de naam en gegevens van de juridische entiteit van Exide (en indien van toepassing van andere voor de verwerking verantwoordelijke entiteiten);

9.1.2 het doel van de verwerking;

9.1.3 een beschrijving van de categorieën van gegevenssubjecten en categorieën van persoonsgegevens;

9.1.4 categorieën van ontvangers van persoonsgegevens;

9.1.5 indien van toepassing gegevens van overdrachten aan derde landen waaronder documentatie over de bestaande waarborgen voor het overdrachtsmechanisme;

9.1.6 waar mogelijk schema's voor documentbehoud; en

9.1.7 indien van toepassing een beschrijving van de technische en organisatorische veiligheidsmaatregelen.

9.2 Als onderdeel van onze documentatie van de verwerkingsactiviteiten documenteren wij of koppelen wij naar documentatie over:

9.2.1 informatie die vereist is voor privacyverklaringen;

9.2.2 gegevens van toestemming;

9.2.3 overeenkomsten met voor de verwerking verantwoordelijke entiteiten-verwerkers

9.2.4 de locatie van de persoonlijke informatie

9.2.5 DPIA's; en

9.2.6 gegevens van gegevensinbreuken.

9.3 Als wij gevoelige persoonlijke informatie of informatie van het strafregister verwerken, bewaren wij schriftelijke dossiers van:

9.3.1 het/de relevante doel(en) waarvoor de verwerking plaatsvindt, met inbegrip van (indien vereist) waarom het nodig is;

9.3.2 de rechtmatige basis voor onze verwerking; en

9.3.3 of wij de persoonlijke informatie bewaren of verwijderen in overeenkomst met ons beleidsdocument en als dat niet het geval is de redenen voor het niet opvolgen van ons beleid.

9.4 Wij zullen de door ons verwerkte persoonlijke informatie regelmatig evalueren en onze documentatie overeenkomstig bijwerken.

10 Rechten van gegevenssubjecten

10.1 Gegevenssubjecten hebben met betrekking tot hun persoonlijke informatie de volgende rechten:

10.1.1 om te worden geïnformeerd over hoe, waarom en op welke basis die informatie wordt verwerkt—zie Exide's *[kennisgevingen inzake gegevensbescherming];*

10.1.2 om de bevestiging te krijgen dat hun informatie wordt verwerkt en er toegang toe te verkrijgen en bepaalde andere informatie door het indienen van een toegangsaanvraag;

10.1.3 om de gegevens te laten corrigeren indien deze onnauwkeurig of onvolledig is;

10.1.4 om de gegevens te laten verwijderen als deze niet langer nodig zijn voor het doel waarvoor zij oorspronkelijk werden verzameld/verwerkt of als er geen doorslaggevende legitieme redenen zijn voor de verwerking (dit wordt soms 'het recht om te worden vergeten' genoemd);

10.1.5 om de verwerking van persoonlijke informatie te beperken wanneer de nauwkeurigheid van de informatie wordt betwijfeld of wanneer de verwerking onrechtmatig is; en

10.1.6 om de verwerking van persoonlijke informatie tijdelijk te beperken wanneer zij menen dat deze onnauwkeurig is of wanneer zij bezwaar hebben gemaakt tegen de verwerking;

10.1.7 om waar wettelijk vereist richtlijnen te verschaffen voor de bewaring, verwijdering en communicatie van hun persoonlijke informatie na hun overlijden.

11 Plichten van gegevenssubjecten

11.1 Iedereen is verplicht om Exide te helpen hun persoonlijke informatie up-to-date te houden. Tijdens uw dienstverband of vanaf uw indienstneming hebt u mogelijk toegang tot de persoonlijke informatie van andere werknemers, leveranciers en klanten. In dat geval verwacht de vennootschap dat u voldoet aan haar verplichtingen inzake gegevensbescherming ten aanzien van die gegevenssubjecten. Als u toegang hebt tot persoonlijke gegevens, moet u:

11.1.1 uitsluitend toegang krijgen tot de persoonlijke informatie waartoe u bevoegd bent en uitsluitend voor toegestane doeleinden;

11.1.2 uitsluitend ander personeel van Exide toegang verlenen tot persoonlijke informatie indien deze over de juiste bevoegdheid beschikken;

11.1.3 personen die geen personeel zijn van de vennootschap uitsluitend toegang verlenen tot persoonlijke informatie als u daartoe specifieke bevoegdheid hebt van de Human Resources- of juridische afdeling;

11.1.4 persoonlijke informatie veilig te bewaren (bijvoorbeeld door te voldoen aan de voorschriften voor toegang tot gebouwen, computers, wachtwoordbeveiliging en veilige opslag en vernietiging en andere voorzorgsmaatregelen zoals uiteengezet in het wereldwijde beleid inzake informatiebeveiliging van de vennootschap);

11.1.5 geen persoonlijke informatie of apparaten met persoonlijke informatie (of welke kunnen worden gebruikt om toegang te verkrijgen) uit de gebouwen van de vennootschap verwijderen tenzij er passende veiligheidsmaatregelen zijn getroffen (zoals pseudonimisering, versleuteling of wachtwoordbeveiliging) om de informatie en het apparaat te beveiligen; en

11.1.6 geen persoonlijke informatie opslaan op lokale schijven of op persoonlijke apparaten die voor werkdoeleinden worden gebruikt.

11.2 U dient contact op te nemen met de afdeling Human Resources of de juridische afdeling als u zich zorgen maakt of vermoedt dat één van de volgende feiten heeft plaatsgevonden (of plaatsvindt of waarschijnlijk zal plaatsvinden):

11.2.1 de verwerking van persoonlijke informatie zonder wettelijke basis voor de verwerking of in geval van gevoelige persoonlijke informatie;

11.2.2 elke inbreuk zoals uiteengezet in paragraaf 15.1 hieronder;

11.2.3 toegang tot persoonlijke informatie zonder voorafgaande toestemming;

11.2.4 persoonlijke informatie die niet veilig wordt bewaard of verwijderd;

11.2.5 de verwijdering van persoonlijke informatie of apparaten met persoonlijke informatie (of die kunnen worden gebruikt om toegang te verkrijgen) uit de gebouwen van de vennootschap zonder passende veiligheidsmaatregelen;

11.2.6 elke andere inbreuk op dit beleid of één van de beginselen van gegevensbescherming zoals uiteengezet in paragraaf 4.1 hierboven.

12 Toegang voor gegevenssubjecten

12.1 Een gegevenssubject mag op elk gewenst moment een verzoek (“SAR”) indienen om meer informatie te verkrijgen over de persoonlijke informatie die de vennootschap over hem/haar bewaart. De vennootschap is normaal gesproken verplicht om binnen één maand na ontvangst op SAR’s te reageren (dit kan worden vereist tot maximaal twee maanden in geval van complexe en/of talrijke verzoeken en in dergelijke gevallen wordt het gegevenssubject geïnformeerd over de behoefte van een verlenging).

12.2 Alle ontvangen verzoeken om toegang tot het onderwerp te verkrijgen moeten worden doorgestuurd naar de lokale AVG-correspondent.

12.3 De vennootschap brengt geen kosten in rekening voor de verwerking van normale SAR’s. Exide behoudt zich het recht voor om redelijke kosten in rekening te brengen voor extra afschriften van informatie die reeds aan een gegevenssubject is verstrekt of voor verzoeken die duidelijk ongegrond of buitensporig zijn, met name wanneer dergelijke verzoeken herhaaldelijk worden gedaan.

13 Informatiebeveiliging

13.1 De vennootschap gebruikt passende technische en organisatorische maatregelen om persoonlijke informatie te beveiligen, en met name te beschermen tegen ongeoorloofde of onwettige verwerking en tegen accidenteel verlies, vernietiging of schade. Dit kan omvatten:

13.1.1 ervoor zorgen dat waar mogelijk persoonlijke informatie wordt gepseudonimiseerd of versleuteld;

13.1.2 het waarborgen van 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 van en toegang tot persoonlijke informatie 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 veiligheid van de verwerking te waarborgen.

13.2 Wanneer de vennootschap namens haarzelf gebruik maakt van externe organisaties voor het verwerken van persoonlijke informatie, moeten er aanvullende veiligheidsmaatregelen worden opgenomen in de overeenkomsten met deze organisaties om de veiligheid van persoonlijke informatie te waarborgen. Met name overeenkomsten met externe organisaties moeten daarin voorzien;

13.2.1 de organisatie mag uitsluitend handelen op basis van schriftelijke instructies van Exide;

13.2.2 degenen die belast zijn met het verwerken van de gegevens zijn onderworpen aan een geheimhoudingsplicht;

13.2.3 er worden passende maatregelen getroffen om de veiligheid van de verwerking te waarborgen;

13.2.4 onderaannemers worden uitsluitend ingeschakeld met de voorafgaande toestemming van Exide en op basis van een schriftelijke overeenkomst;

13.2.5 de organisatie helpt Exide om de gegevenssubjecten toegang te verlenen en in staat te stellen om hun rechten met betrekking tot gegevensbescherming uit te oefenen;

13.2.6 de organisatie helpt Exide bij het naleven van haar verplichtingen met betrekking tot de veiligheid van de verwerking, de berichtgeving van inbreuken op de gegevens en de beoordeling van de gevolgen van gegevensbescherming;

13.2.7 de organisatie zal alle persoonlijke informatie verwijderen of aan Exide retourneren zoals verzocht aan het eind van de overeenkomst;

13.2.8 de organisatie onderwerpt zich aan audits en inspecties en Exide voorzien van alle informatie die de vennootschap nodig heeft om te waarborgen dat zowel Exide als de organisatie aan hun verplichtingen inzake gegevensbescherming voldoen; en

13.2.9 de organisatie informeert Exide onmiddellijk als haar wordt gevraagd om iets te doen dat in strijd is met de wet op gegevensbescherming.

13.3 Voordat een nieuwe overeenkomst met betrekking tot de verwerking van persoonlijke informatie door een externe organisatie wordt gesloten of dat een bestaande overeenkomst wordt veranderd, moet het desbetreffende personeel de voorwaarden van deze overeenkomst door de juridische afdeling van Exide laten goedkeuren.

14 Opslag en instandhouding van persoonlijke informatie

14.1 Persoonlijke informatie (en gevoelige persoonlijke informatie) wordt veilig bewaard in overeenstemming met het wereldwijde beleid inzake informatiebeveiliging van de vennootschap.

14.2 Persoonlijke informatie (en gevoelige persoonlijke informatie) dient niet langer bewaard te worden dan noodzakelijk. Hoe lang gegevens moeten worden bewaard is afhankelijk van de omstandigheden, met inbegrip van de redenen waarvoor de persoonlijke informatie werd verkregen. Werknemers zijn verplicht het beleid inzake gegevensbewaring van de vennootschap waarin de desbetreffende bewaartermijn wordt uiteengezet op te volgen of de criteria die moeten worden gebruikt om de bewaartermijn te bepalen. Bij onzekerheid dient het personeel de lokale AVG-correspondent of de juridische afdeling te raadplegen.

15 Inbreuken in verband met persoonsgegevens

15.1 Een gegevensinbreuk kan veel verschillende vormen aannemen, bijvoorbeeld:

15.1.1 verlies of diefstal van gegevens of apparatuur waarop persoonlijke informatie wordt opgeslagen;

15.1.2 ongeoorloofde toegang tot of gebruik van persoonlijke informatie ofwel door een personeelslid of externe partij;

15.1.3 verlies van gegevens als gevolg van een defect aan de apparatuur of systemen (inclusief hardware en software);

15.1.4 menselijke fout zoals het onbedoeld verwijderen of veranderen van gegevens;

15.1.5 onvoorziene omstandigheden zoals brand of wateroverlast;

15.1.6 moedwillige aanvallen op IT-systemen zoals hacken, virussen of phishing; en

15.1.7 wanneer informatie wordt verkregen door het misleiden van de organisatie die deze informatie in bezit heeft.

15.2 De vennootschap zal:

15.2.1 zonder onnodige vertraging de verplichte melding van gegevensinbreuk aan de desbetreffende toezichthoudende autoriteit of het Information Commissioner's Office (VK) melden, en waar mogelijk binnen 72 uur na kennisname van de melding, als het waarschijnlijk een risico voor de rechten en vrijheden van gegevenssubjecten met zich meebrengt; en

15.2.2 de betrokken gegevenssubjecten informeren wanneer een gegevensinbreuk waarschijnlijk leidt tot een risico voor hun rechten en vrijheden en waar kennisgeving bij wet verplicht is.

16 Internationale overdrachten

16.1 De vennootschap kan persoonlijke informatie buiten de Europese Economische Ruimte (EER) (die de landen van de Europese Unie en IJsland, Liechtenstein en Noorwegen omvat) overdragen aan de uiteindelijke moedermaatschappij van de vennootschap, Exide Technologies in de Verenigde Staten van Amerika, op voorwaarde dat Exide Technologies is aangewezen als onderneming die over standaardclausules inzake gegevensbescherming beschikt.

17 Opleiding

De vennootschap zorgt ervoor dat het personeel voldoende is opgeleid met betrekking tot hun verantwoordelijkheden inzake gegevensbescherming. Personen wiens functies regelmatig toegang vereisen tot persoonlijke informatie of die verantwoordelijk zijn voor de uitvoering van dit

beleid of krachtens dit beleid verzoeken tot toegang van de subjecten beantwoorden, ontvangen aanvullende opleiding waarmee zij inzicht krijgen in hun taken en de manier waarop zij daaraan kunnen voldoen.

18 Gevolgen van niet-naleving

18.1 De vennootschap neemt het naleven van dit beleid uiterst serieus. Het niet naleven van dit beleid:

18.1.1 brengt de gegevenssubjecten waarvan de persoonlijke informatie wordt verwerkt in gevaar; en

18.1.2 brengt het risico met zich mee van aanzienlijke civielrechtelijke sancties voor de persoon en de vennootschap; en

18.1.3 kan in sommige omstandigheden leiden tot een strafbaar feit.

18.2 Gezien het belang van dit beleid kan het niet naleven van een verplichting door een werknemer op grond van onze procedures leiden tot disciplinaire maatregelen en deze handeling kan leiden tot ontslag wegens ernstig wangedrag. Als iemand die geen werknemer is dit beleid overtreedt, kan zijn overeenkomst met onmiddellijk ingang worden beëindigd.

18.3 Aarzel bij vragen of twijfels over dit beleid niet om contact op te nemen met de landelijk vertegenwoordiger inzake AVG of met de juridische afdeling.