ARBONIA

Richtlijn over de omgang met persoonsgegevens (Richtlijn inzake gegevensbescherming)

16. juni 2020

ARBONIA

INHOUDSOPGAVE

ARBONIA

1 DOEL

Het is essentieel om persoonsgegevens te verzamelen en te verwerken om aan wettelijke en contractuele verplichtingen te voldoen. De voorschriften inzake gegevensbescherming die gelden in de betreffende landen moeten in acht worden genomen. Deze richtlijn beschrijft hoe Arbonia AG en haar groepsondernemingen (hierna gezamenlijk "Arbonia", of een individuele groepsonderneming, hierna "groepsonderneming" genoemd) omgaan met persoonsgegevens. De vastgestelde bepalingen gelden als minimumnormen. Als de lokale wet op de gegevensbescherming strengere voorschriften voorziet, moeten deze in acht worden genomen. Eventuele lokale voorschriften voor de uitvoering van deze richtlijn moeten ook in acht worden genomen.

Het doel van deze richtlijn inzake de verwerking van gegevens ("gegevensbeschermingsrichtlijn") is het bepalen, implementeren, handhaven en continu verbeteren van de naleving van de gegevensbescherming, in overeenstemming met de eisen van de Algemene Verordening Gegevensbescherming 2016/679 van de Europese Unie (de **AVG**) en alle andere toepasselijke lokale wetten inzake gegevensbescherming (samen de **toepasselijke wetten inzake gegevensbescherming** genoemd) door Arbonia.

Door het niet-naleven van de toepasselijke wetgeving inzake gegevensbescherming loopt Arbonia het risico van op reputatieschade en zware boetes (bijvoorbeeld tot 4% van zijn wereldwijde omzet krachtens de AVG). Het kan onze klanten en medewerkers ook blootstellen aan bepaalde privacyrisico's, zoals identiteitsdiefstal of financieel verlies. Naleving van de toepasselijke wetgeving inzake gegevensbescherming helpt ons het vertrouwen in de Arbonia-organisatie te behouden en een succesvolle bedrijfsvoering te garanderen.

De doelstelling van deze gegevensbeschermingsrichtlijn is het kader te bieden voor een dergelijke naleving van de gegevensbescherming binnen Arbonia. De richtlijn is met name bedoeld om de basisbeginselen voor de verwerking van persoonsgegevens (de **gegevensbeschermingsbeginselen**), die in punt 6 zijn opgenomen en die verantwoordelijk zijn voor de ondernemingen van Arbonia wanneer zij als verantwoordelijke partij optreden in het kader van de AVG, te implementeren, regelt de noodzaak van passende technische en organisatorische maatregelen en het melden van incidenten op het gebied van gegevensbescherming als minimumnorm voor alle ondernemingen van Arbonia, en is van toepassing op alle werknemers van Arbonia en de leden van de Raad van Bestuur van Arbonia AG.

Het biedt ook een kader voor verdere eisen die van toepassing zijn op verwerkingsverantwoordelijken en verwerkers in het kader van de AVG (of soortgelijke toepasselijke wetgeving inzake gegevensbescherming), zoals beschreven in punt 7.

ARBONIA

2 TERMEN EN DEFINITIES

In het kader van deze richtlijn inzake gegevensbescherming zijn de volgende termen en definities van toepassing:

Anonieme gegevens betekenen dat de persoonlijke identiteit nooit door iemand kan worden opgespoord of dat de persoonlijke identiteit alleen met onredelijke tijd, kosten en moeite kan worden opgespoord.

De toepasselijke wetgeving inzake gegevensbescherming staat voor de basisverordening inzake gegevensbescherming van de Europese Unie 2016/679 (de **AVG**) of enige andere toepasselijke nationale wetgeving inzake gegevensbescherming die soortgelijke bepalingen bevat.

Bedrijfsproceseigenaar staat voor een natuurlijk persoon die een verantwoordelijke persoon is onder deze richtlijn en die verantwoordelijk is voor de verwerking van persoonsgegevens en de respectievelijke IT-toepassing.

Onder **toestemming** wordt verstaan de toestemming van de betrokkene, dat wil zeggen elke vrijwillig gegeven, geïnformeerde en ondubbelzinnige uiting van zijn of haar wensen in de vorm van een verklaring of een andere ondubbelzinnige bevestigende handeling waarmee de betrokkene zijn of haar instemming met de verwerking van de hem of haar betreffende persoonsgegevens kenbaar maakt.

Verwerkingsverantwoordelijke staat voor de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of een andere instantie die alleen of samen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Onder **gegevensbeveiligingsincident** wordt verstaan een gebeurtenis die aanleiding geeft tot een redelijk vermoeden dat persoonsgegevens op onrechtmatige wijze worden verzameld, verzameld, gewijzigd, gekopieerd, doorgegeven of gebruikt. Dit kan betrekking hebben op handelingen van derden of werknemers.

Onder **betrokkene** wordt een geïdentificeerde of identificeerbare natuurlijke persoon verstaan. Een identificeerbare natuurlijke persoon is een persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatiemiddel zoals een naam, een identificatienummer, locatiegegevens, een online-identificatiemiddel of één of meer factoren die specifiek zijn voor de fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit van die natuurlijke persoon.

De **verwerker** is een natuurlijke of rechtspersoon, een overheidsinstantie, een agentschap of een andere instantie die namens de voor de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Lijst van verwerkingsprocessen: registratie van de gegevensverwerking onder de verantwoordelijkheid van de verwerkingsverantwoordelijke. Deze lijst bevat alle onderstaande gegevens: (i) de naam en de contactgegevens van de verwerkingsverantwoordelijke en, indien van toepassing, de gezamenlijke verwerkingsverantwoordelijken, de vertegenwoordiger van de verwerkingsverantwoordelijke en de plaatselijke coördinator voor gegevensbescherming; (ii) de doeleinden van de verwerking; (iii) een beschrijving van de categorieën betrokkenen en de categorie persoonsgegevens; (iv) de categorieën ontvangers aan wie persoonsgegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen; (v) indien van toepassing, de doorgifte van persoonsgegevens aan een derde land, met inbegrip van de identificatie van het derde land en de documentatie van passende waarborgen; (vi) de beoogde termijnen voor het verwijderen van de verschillende categorieën persoonsgegevens; (vii) een algemene beschrijving van de technische en organisatorische veiligheidsmaatregelen.

De functionaris voor gegevensbescherming of de gegevensbeschermingscoördinator of CGB staat voor de in punt 5 beschreven persoon.

Persoonsgegevens staat voor alle informatie (met inbegrip van persoonsgegevens van bijzondere categorieën) met betrekking tot de betrokkene, dus met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon, zoals naam, geboortedatum, e-mailadres, religie, locatiegegevens, online gegevens (IP-adres, locatiegegevens, enz.), identificatienummers (sofi-nummer, identiteitskaartnummer, enz.), fysieke kenmerken (geslacht, huidskleur, haarkleur, oogkleur, etc.), klantgegevens, etc.), die onderworpen zijn aan een geldende regelgeving op het gebied van gegevensbescherming.

Verwerking of verwerken staat voor elke bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Pseudonimisering staat voor de verwerking van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet langer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.

Persoonsgegevens van bijzondere categorieën staat voor gegevens waaruit ras of etnische afkomst, politieke opvattingen, religie of levensbeschouwelijke overtuigingen, strafrechtelijke veroordelingen, vakbondslidmaatschap, gezondheid of seksuele geaardheid van de betrokkene of genetische gegevens blijken, biometrische gegevens met het oog op de ondubbelzinnige identificatie van een natuurlijke persoon.

Derde landen zijn alle landen die geen land zijn van de Europese Unie of de Europese Economische Ruimte of een land met een adequaat niveau van gegevensbescherming dat door de Europese Commissie als adequaat wordt beschouwd (zie de lijst van landen met een adequaat niveau van gegevensbescherming):
< https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Onder **derde** wordt verstaan eenieder die niet de betrokkene, de verwerkingsverantwoordelijke of de verwerker is (met inbegrip van bijvoorbeeld zakenpartners, onderaannemers, kredietinformatiebureaus en anderen), alsmede personen die gemachtigd zijn om onder het rechtstreekse gezag van de verwerkingsverantwoordelijke of de verwerker persoonsgegevens te verwerken. Bij de verwerking van persoonsgegevens onder een vergunning zijn verwerkers volgens de wet op de gegevensbescherming geen wettelijke derden, aangezien zij wettelijk aan de verwerkingsverantwoordelijke worden toegerekend.

3 OMVANG

3.1 Organisatorische omvang

Deze richtlijn inzake gegevensbescherming geldt voor alle groepsondernemingen van Arbonia, alle werknemers van Arbonia en de leden van de Raad van Bestuur van Arbonia AG. Ze moet op een juridisch bindende manier in elke groepsonderneming worden geïmplementeerd.

3.2 Wetten, verordeningen, normen en richtlijnen

Deze gegevensbeschermingsrichtlijn omvat de vereisten van de AVG en de internationaal erkende gegevensbeschermingsbeginselen, zonder de bestaande nationale wetgeving te vervangen. Het is een aanvulling op de nationaal geldende wetgeving inzake gegevensbescherming. In geval van strijdigheid tussen de nationale wetgeving en deze richtlijn inzake gegevensbescherming of indien de eisen strenger zijn, dan derogeert deze richtlijn aan de desbetreffende nationale wetgeving. De inhoud van deze richtlijn inzake gegevensbescherming moet worden nageleefd, zelfs als er geen overeenkomstige nationale wetgeving bestaat.

Indien deze richtlijn inzake gegevensbescherming in strijd is met de regelgeving in een bepaald land, kunnen de specifieke bepalingen van deze richtlijn worden aangenomen in een lokale richtlijn in overleg met het hoofd van Legal & Compliance. De wezenlijke inhoud en het doel van de betrokken bepalingen mogen echter niet worden gewijzigd.

ARBONIA

4 REGELGEVENDE BASIS

Deze gegevensbeschermingsrichtlijn is gebaseerd op de AVG en de wereldwijd aanvaarde basisbeginselen van gegevensbescherming.

5 ROLLEN EN VERANTWOORDELIJKHEDEN

- De gedelegeerd bestuurder van een groepsonderneming[1] is verantwoordelijk:
  1. Er uiteindelijk voor te zorgen dat de betrokken rechtspersoon zijn wettelijke verplichtingen met betrekking tot de verwerking van persoonsgegevens nakomt.
  2. Ervoor te zorgen dat aan de eisen van deze richtlijn inzake gegevensbescherming wordt voldaan (met inbegrip van melding in het geval van incidenten op het gebied van gegevensbeveiliging).
  3. Ervoor te zorgen dat de "lijst van verwerkingsprocessen" op het niveau van de groepsonderneming wordt aangevuld en onderhouden door de bedrijfsproceseigenaar.
  4. Een formele plaatselijke functionaris voor gegevensbescherming (intern of extern) te benoemen (hierna "functionaris voor gegevensbescherming" genoemd) wanneer dit wordt vereist krachtens de lokaal geldende regelgeving inzake gegevensbescherming en deze benoeming jaarlijks halverwege het jaar bekend te maken aan het hoofd van Legal & Compliance en de afdeling Internal Audit.
  5. Een lokale functionaris voor gegevensbescherming (hierna "coördinator voor gegevensbescherming" genoemd) aan te stellen wanneer de lokaal geldende gegevensbeschermingsverordening geen formele lokale functionaris voor gegevensbescherming vereist. Deze benoemde persoon moet jaarlijks halverwege het jaar aan het hoofd van Legal & Compliance en Internal Audit worden bekendgemaakt.

- De door de gedelegeerd bestuurder van een groepsonderneming aangestelde[2] lokale coördinator voor gegevensbescherming of functionaris voor gegevensbescherming moet:
  1. Toezien op de naleving van deze richtlijn inzake gegevensbescherming en de instructies van de verwerkingsverantwoordelijke of de verwerker met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de delegatie van verantwoordelijkheden en de bijbehorende controles.
  2. De verwerkingsverantwoordelijke of de verwerker en de werknemers die de verwerkingsverplichtingen in het kader van deze richtlijn uitvoeren, informeren, adviseren en begeleiden.
  3. Op vraag advies geven over een privacyeffectbeoordeling voor persoonsgegevens en de resultaten daarvan bewaken en andere vragen beantwoorden over de

[1] Voor niet-operationeel actieve groepsondernemingen wordt deze verantwoordelijkheid afzonderlijk bepaald in overleg met het hoofd van Legal & Compliance.
[2] Voor niet-operationeel actieve groepsondernemingen wordt deze verantwoordelijkheid afzonderlijk bepaald in overleg met het hoofd van Legal & Compliance.

persoonsgegevens die hem in het kader van deze richtlijn inzake gegevensbescherming zijn toegewezen.

4. De "lijst van verwerkingsprocessen", die wordt bijgehouden door de betreffende groepsonderneming en ingevuld door de bedrijfsproceseigenaars bewaken en bijhouden en de volledigheid en actualiteit van de lijst jaarlijks halverwege het jaar aan de Gedelegeerd Bestuurder en het hoofd van Legal & Compliance bevestigen.
5. Dienen als aanspreekpunt voor het hoofd van Legal & Compliance en hem op de hoogte houden van de verantwoordelijkheden, risico's en problemen met betrekking tot de bescherming van persoonsgegevens.
6. De IT-afdeling die verantwoordelijk is voor de IT-applicaties helpen bij het beoordelen en goedkeuren van nieuwe IT-applicaties op niveau van de groepsonderneming voor de verwerking van persoonsgegevens en elke IT-applicatie voor de verwerking van bijzondere categorieën van persoonsgegevens vanuit het oogpunt van gegevensbescherming.
7. Toestemming geven voor de doorgifte van persoonsgegevens aan een derde land vanuit het oogpunt van gegevensbescherming (zie ook hieronder, punt 14).
8. Optreden als lokale contactpersoon voor de toezichthoudende autoriteit met betrekking tot kwesties op het gebied van gegevensverwerking, en met de toezichthoudende autoriteit samenwerken.
9. Het behandelen van verzoeken van medewerkers die betrokken zijn bij de verwerking van persoonsgegevens.
10. Het beantwoorden van verzoeken van betrokkenen om informatie over persoonsgegevens die in het bezit zijn van Arbonia, of in het geval van een verzoek dat betrekking heeft op meerdere groepsondernemingen van Arbonia, deze verzoeken behandelen in coördinatie met Corporate IT (zie ook hieronder, punt 7.4)
11. Het beoordelen en goedkeuren van contracten of overeenkomsten met de verwerker die zijn opgesteld of vooraf zijn beoordeeld door de eigenaar van het bedrijfsproces en die namens Arbonia persoonsgegevens kunnen verwerken zoals beschreven in artikel 7.2.
12. Toezicht houden op de externe plaatselijke functionaris voor gegevensbescherming, indien deze is aangesteld.
13. Het melden van incidenten op het gebied van gegevensbeveiliging overeenkomstig de Data Breach Notification-richtlijn (zie punt 9 evenals het "Arbonia Data Breach Policy").

- De IT-directie is samen met Corporate IT verantwoordelijk voor:
  1. Het definiëren van de normen die van toepassing zijn op de hele Groep en de algemene IT-controles (GITC) die in acht moeten worden genomen bij de opslag van gegevens.

- De IT-afdeling die verantwoordelijk is voor een groepsonderneming is verantwoordelijk voor:
  1. Door middel van passende normen, beleidsmaatregelen en de uitvoering van algemene IT-controles (GITC) ervoor zorgen dat de systemen, diensten en

apparatuur voor de opslag van gegevens voldoen aan aanvaardbare veiligheidsnormen (toegangscontrole/verwijdering van gegevens), rekening houdend met de stand van de techniek, de kosten van de uitvoering en de aard, de reikwijdte, de context en het doel van de verwerking, alsmede met de uiteenlopende waarschijnlijkheidsgraad en de ernst van de gevolgen voor de rechten en vrijheden van natuurlijke personen.

2. Ernaar streven dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen treffen om een beschermingsniveau te waarborgen dat in overeenstemming is met het risico, zoals bepaald in punt 8.
3. Na raadpleging van de coördinator voor gegevensbescherming of de functionaris voor gegevensbescherming nieuwe IT-toepassingen voor de verwerking van persoonsgegevens vanuit het oogpunt van gegevensbescherming onderzoeken en goedkeuren.
4. Het uitvoeren van regelmatige controles en scans om ervoor te zorgen dat de veiligheidshardware en -software naar behoren functioneert. De resultaten van de gegevensbeschermingscontroles moeten aan de bevoegde functionaris voor gegevensbescherming worden gemeld.
5. Het beoordelen van de gegevensbeveiliging van diensten van derden (bijv. opdrachtverwerkers) die het bedrijf kan overwegen te gebruiken om persoonsgegevens te verwerken (bijv. cloud computingdiensten, enz.)
6. Een lijst van gegevensbeveiligingsincidenten bijhouden en gegevensbeveiligingsincidenten melden aan Corporate IT.
7. Het coördineren en beantwoorden van verzoeken van betrokkenen om informatie over persoonsgegevens die in het bezit zijn van de groepsonderneming van Arbonia, ondersteund door de respectieve IT-afdeling (zie ook het volgende punt 7.4)
8. Eventuele incidenten of risico's die worden ontdekt op het gebied van gegevensbeveiliging melden overeenkomstig de richtlijn betreffende de melding van inbreuken op de gegevensbescherming (zie punt 9 evenals het "Arbonia Data Breach Policy“)

- Corporate IT, in samenwerking met de IT-afdeling die verantwoordelijk is voor de ondersteuning van een groepsonderneming, is verantwoordelijk voor:
  1. Het uitvoeren van regelmatige controles en scans om ervoor te zorgen dat de veiligheidshardware en -software naar behoren functioneert. De resultaten van de gegevensbeschermingscontroles moeten aan de bevoegde functionaris voor gegevensbescherming worden gemeld.
  2. Een centrale lijst van incidenten op het gebied van gegevensbeveiliging bijhouden.
  3. Eventuele incidenten of risico's die worden ontdekt op het gebied van gegevensbeveiliging melden overeenkomstig de richtlijn betreffende de melding van inbreuken op de gegevensbescherming (zie punt 9 evenals het "Arbonia Data Breach Policy").

- Internal Audit is verantwoordelijk voor:

1. In het kader van een op risicoanalyse gebaseerde controle, die volgens de reguliere controleplanning wordt uitgevoerd, nagaan of de organisatorische procedures voldoen aan de essentiële eisen van deze richtlijn inzake gegevensbescherming.

- De bedrijfsproceseigenaar:
  1. Dient evoor te zorgen dat de plaatselijke functionaris voor gegevensbescherming op passende wijze en tijdig wordt betrokken bij alle zaken die nodig zijn om de verwerking van persoonsgegevens te beoordelen.
  2. Is verantwoordelijk voor het opstellen of vooraf beoordelen van alle contracten of overeenkomsten met de verwerker die namens Arbonia persoonsgegevens kan verwerken zoals beschreven in punt 7.2.
  3. De "lijst van verwerkingsprocessen" in te vullen en bij te houden, die wordt bijgehouden door de desbetreffende groepsonderneming, en de volledigheid en actualiteit van de gegevens jaarlijks eind april te bevestigen aan de coördinator voor gegevensbescherming of de functionaris voor gegevensbescherming.
  4. Alvorens nieuwe verwerkingen van persoonsgegevens uit te voeren, moeten de daaruit voortvloeiende risico's voor de persoonlijkheid en de grondrechten van de betrokkene worden beoordeeld en moet, wanneer het risico van verwerking waarschijnlijk groot is, vooraf een effectbeoordeling voor de gegevensbescherming worden uitgevoerd.

6 GEGEVENSBESCHERMINGSBEGINSELEN VOOR DE VERWERKING VAN PERSOONSGEGEVENS

Elke groepsonderneming die als verwerkingsverantwoordelijke optreedt, moet ervoor zorgen dat zij kan aantonen dat zij de volgende **6 (zes) belangrijkste beginselen inzake gegevensbescherming in acht neemt**:

1. Persoonsgegevens alleen verwerken indien een geldige rechtsgrond volgens de toepasselijke wetgeving inzake gegevensbescherming kan worden aangetoond en de betrokken persoon wordt geïnformeerd over de identiteit en de contactgegevens van de verantwoordelijke persoon, het type en de rechtsgrond van de verzamelde persoonsgegevens, de respectieve bewaartermijnen en het doel waarvoor de persoonsgegevens worden verzameld

2. Altijd het doel eerbiedigen waarvoor de persoonsgegevens werden verzameld

3. Alleen persoonsgegevens verzamelen/verwerken die echt nodig zijn

4. Zorgen dat persoonsgegevens correct blijven en onjuiste persoonsgegevens wissen

5. Persoonsgegevens alleen bewaren gedurende de wettelijke bewaartermijnen die echt nodig zijn

ARBONIA

6. Persoonsgegevens vertrouwelijk behandelen en alleen delen wat echt moet worden gedeeld

6.1 Rechtvaardigheid, wettigheid en transparantie

Persoonsgegevens mogen alleen worden verwerkt voor specifiek toegestane doeleinden zoals hieronder beschreven en op een transparante manier. Persoonsgegevens moeten daarom op een wettige en eerlijke manier worden verwerkt en de individuele rechten van de betrokken personen moeten worden gerespecteerd. Het kan daarbij gaan om persoonsgegevens die Arbonia rechtstreeks van een betrokkene ontvangt (bijvoorbeeld door het invullen van formulieren of door correspondentie met ons per post, telefoon, e-mail of anderszins), maar ook om persoonsgegevens die Arbonia van derden ontvangt.

Op grond van de toepasselijke wetgeving inzake gegevensbescherming kunnen persoonsgegevens rechtmatig worden verwerkt op basis van een van de **vijf gerechtvaardigde redenen** (de **gerechtvaardigde redenen**) in overeenstemming met de AVG. Deze redenen zijn:

1. **Contract**: De verwerking van persoonsgegevens is noodzakelijk voor de uitvoering van een contract waarbij de betrokkene partij is of voor de uitvoering van precontractuele maatregelen die op verzoek van de betrokkene zijn genomen, of

2. **Toestemming**: De verwerking van persoonsgegevens is gebaseerd op de toestemming (opt-in model) van de betrokkene voor een of meer specifieke doeleinden. De toestemming moet worden gedocumenteerd, of

3. **Wettelijke verplichting**: De verwerking van persoonsgegevens is gebaseerd op een wettelijke verplichting van Arbonia. De aard en de omvang van de gegevensverwerking moet noodzakelijk zijn voor de wettelijk toegestane verwerkingsactiviteit en in overeenstemming zijn met de toepasselijke wettelijke voorwaarden, of

4. **Het algemeen belang**: De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of

5. **Gerechtvaardigde zakelijke belangen**: De verwerking van persoonsgegevens wordt geacht in verhouding te staan tot de gerechtvaardigde zakelijke belangen van Arbonia of van de derde aan wie de persoonsgegevens worden verstrekt, tenzij de belangen of fundamentele rechten en vrijheden van de betrokkene zwaarder wegen dan deze belangen. Gerechtvaardigde belangen zijn van algemene juridische aard (bijv. inning van openstaande vorderingen / door middel van een collectieve

overeenkomst met de ondernemingsraad / bewaring/uitoefening of verweer tegen wettelijke aanspraken met betrekking tot de betrokkene) of commerciële aard (bijv. het vermijden van contractbreuk).

De transparantie vereist dat de betrokkene op de hoogte wordt gebracht van de wijze waarop met zijn of haar persoonsgegevens wordt omgegaan. Daarom wordt in het algemeen aanbevolen om de persoonsgegevens rechtstreeks bij de betrokkene te verzamelen (en niet via een derde). Bij de verwerking van persoonsgegevens moet de betrokkene op de hoogte worden gesteld van het volgende:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke en, in voorkomend geval, zijn vertegenwoordiger in de EU,
- in voorkomend geval, de contactgegevens van de coördinator of de functionaris voor gegevensbescherming,
- het doel van de verwerking van de persoonsgegevens en de rechtsgrondslag voor de verwerking,
- derde ontvangers of categorieën derde ontvangers aan wie gegevens kunnen worden doorgegeven,
- indien van toepassing, informatie over de verwerking in een derde land en verwijzing naar adequate waarborgen.

6.2 Doelbinding

Persoonsgegevens mogen alleen worden verwerkt voor het doel dat aan de betrokkene is medegedeeld voordat de persoonsgegevens worden verzameld. Latere wijzigingen van het doel zijn slechts in beperkte mate mogelijk en moeten worden gemotiveerd. De verantwoordelijke dient de betrokkene te informeren over het doel waarvoor Arbonia zijn persoonsgegevens verwerkt wanneer Arbonia de persoonsgegevens voor het eerst verzamelt of zo spoedig mogelijk daarna. Elke verwerking voor reclamedoeleinden of marketingprogramma's moet de betrokkene het recht geven bezwaar te maken tegen de verwerking van zijn persoonsgegevens en hij moet uitdrukkelijk hierover geïnformeerd worden. In dit verband moet elke verantwoordelijke een klachtenbehandelingssysteem invoeren dat ervoor zorgt dat opt-outs worden gerespecteerd.

6.3 Gegevensminimalisering

Verwerk alleen persoonsgegevens die echt nodig zijn. Voordat persoonsgegevens worden verwerkt, moet worden vastgesteld of en in hoeverre de verwerking van persoonsgegevens noodzakelijk is om het doel te bereiken waarvoor ze worden verwerkt. Persoonsgegevens mogen niet van tevoren worden verzameld en opgeslagen voor eventuele toekomstige doeleinden, tenzij dit door de nationale wetgeving wordt vereist of toegestaan.

6.4 Correct en actueel

Persoonsgegevens moeten correct en volledig zijn en, in geval van wijzigingen, worden bijgewerkt. Er worden passende maatregelen genomen om ervoor te zorgen dat onjuiste of onvolledige persoonsgegevens worden gewist, gecorrigeerd, aangevuld of bijgewerkt. Iedereen die met persoonsgegevens werkt, moet daartoe de vereiste stappen nemen (bijv. door de gegevens van een betrokkene te bevestigen wanneer hij/zij belt of door een opgeslagen telefoonnummer uit de databank te verwijderen wanneer de betrokkene er geen gebruik meer van maakt).

6.5 Beperkte bewaringstermijn

Persoonsgegevens mogen slechts gedurende de werkelijk benodigde tijd worden opgeslagen. Persoonsgegevens moeten worden verwijderd zodra ze niet langer nodig zijn voor het beoogde doel, of wanneer de toestemming wordt ingetrokken of het gebruik op grond van een gerechtvaardigd belang wordt tegengeworpen, en Arbonia geen dwingende gerechtvaardigde redenen kan aanvoeren. In sommige gevallen kunnen langere bewaartermijnen ons in staat stellen om persoonlijke informatie langer te bewaren indien dit wettelijk verplicht is (bijvoorbeeld op grond van de fiscale of handelswetgeving), of indien persoonlijke informatie nodig is om vorderingen in rechte te doen gelden, uit te oefenen of te verdedigen.

6.6 Vertrouwelijkheid en gegevensbeveiliging

Persoonsgegevens moeten te allen tijde vertrouwelijk worden behandeld en alleen worden gedeeld, omdat ze echt moeten worden gedeeld. Het principe van "noodzakelijke informatie" is van toepassing, zodat werknemers en derden alleen toegang hebben tot persoonsgegevens indien en voor zover dat nodig is om het doel te bereiken. Dit vereist een zorgvuldig ontworpen concept dat de specifieke toegangsrechten voor elk bedrijfsproces definieert, met inbegrip van de implementatie en goedkeuring van rollen en verantwoordelijkheden (concept van toegangsrechten). Ontvangers van persoonsgegevens moeten worden geïnformeerd over de vertrouwelijkheid van de persoonsgegevens **en moeten een vertrouwelijkheidsovereenkomst/geheimhoudingsovereenkomst sluiten** (die deel kan uitmaken van de arbeidsovereenkomst of een soortgelijke overeenkomst). Uitzondering: De ontvanger is onderworpen aan een professionele of wettelijke geheimhoudingsplicht.

De persoonsgegevens moeten worden beveiligd met passende organisatorische en technische maatregelen om onrechtmatige toegang, onrechtmatige verwerking of openbaarmaking en onopzettelijk verlies, wijziging of vernietiging te voorkomen (zie punt 8).

ARBONIA

7 VERDERE VERPLICHTINGEN OP GROND VAN DE AVG OF ANDERE SOORTGELIJKE TOEPASSELIJKE GEGEVENSBESCHERMINGSVOORSCHRIFTEN

7.1 Principe van verantwoording

Een groepsonderneming van Arbonia die onderworpen is aan de AVG (of een vergelijkbare toepasselijke regelgeving inzake gegevensbescherming) moet ervoor zorgen dat zij de naleving van de toepasselijke wetgeving inzake gegevensbescherming kan aantonen (het principe van de "verantwoordingsplicht"). Daarom moeten deze groepsondernemingen, naast de algemene vereisten van deze richtlijn, de volgende punten implementeren en onderhouden, waarbij de gedelegeerd bestuurder van de betreffende groepsonderneming uiteindelijk verantwoordelijk is voor het verzekeren van de implementatie en het onderhoud:

1. Plaatselijke coördinator voor gegevensbescherming of plaatselijke functionaris voor gegevensbescherming: aanstelling van een specifieke plaatselijke coördinator voor gegevensbescherming of een plaatselijke functionaris voor gegevensbescherming.

2. Beheren van de "lijst van verwerkingsprocessen": Er wordt een lijst gemaakt van de verwerkingsactiviteiten van persoonsgegevens en deze wordt actueel gehouden.

3. Legitimiteitscontrole: De rechtmatige verwerking van persoonsgegevens met inachtneming van de geldige gerechtvaardigde redenen moet worden gecontroleerd, met name bij de verwerking van bijzondere categorieën van persoonsgegevens.

4. Controle van de verwerker: Het sluiten van een overeenkomst met de verwerker of als verwerker bij de verstrekking of ontvangst van persoonsgegevens onder een vergunning overeenkomstig artikel 28 van de AVG.

5. In het geval van gezamenlijke verantwoordelijken voor de verwerking moet in een overeenkomst tussen de gezamenlijke verantwoordelijken voor de verwerking worden voorzien in het kader van artikel 26 van de AVG.

6. Medewerkers van Arbonia moeten worden geïnformeerd over de verwerking van persoonsgegevens.

7.2 Regels voor de verwerker (voornamelijk dienstverlenende partners)

De verwerkingsverantwoordelijke werkt alleen met verwerkers die voldoende garanties bieden dat passende technische en organisatorische maatregelen worden genomen om de verwerking van persoonsgegevens in overeenstemming met de vereisten van artikel 28 van de AVG uit te voeren en de bescherming van de rechten van de betrokkene te waarborgen.

Voor gedeelde diensten binnen Arbonia is er een overeenkomst die het mogelijk maakt om persoonsgegevens door te geven, op voorwaarde dat er legitieme wettelijke redenen zijn om deze persoonsgegevens door te geven in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming.

7.2.1 Verstrekking van persoonsgegevens aan de verwerker (uitgaand)

Verwerking van persoonsgegevens onder een licentie betekent dat een dienstverlener wordt gecontracteerd om persoonsgegevens te verwerken zonder dat hij de verantwoordelijkheid krijgt voor het desbetreffende bedrijfsproces (d.w.z. dienstverleners, uitbestedingsdiensten). In dit geval moet een contract voor de verwerking van persoonsgegevens worden gesloten met externe aanbieders onder een licentie. De desbetreffende groepsonderneming van Arbonia is de verantwoordelijke partij en behoudt de volledige verantwoordelijkheid voor de correcte verwerking van persoonsgegevens door de verwerker.

De desbetreffende eigenaar van het bedrijfsproces moet ervoor zorgen dat de huidige modelovereenkomst voor contractverwerking, of een soortgelijk contract dat door de dienstverlener wordt verstrekt om aan de eisen van artikel 28 AVG te voldoen, wordt gebruikt om dergelijke dienstverleners in dienst te nemen. Een andere mogelijkheid is dat een dienstverlener zijn naleving van de gegevensbeveiligingseisen documenteert door een passende en goedgekeurde EU-certificering in te dienen. Elke afwijking van een dergelijke veiligheidsnorm moet worden goedgekeurd door de functionaris voor gegevensbescherming of de coördinator voor gegevensbescherming in samenwerking met Corporate IT. Bestaande contracten moeten binnen een jaar na de inwerkingtreding van deze richtlijn inzake gegevensbescherming worden herzien en moeten een schriftelijke overeenkomst voor de verwerking van het contract bevatten.

7.2.2 Het ontvangen van persoonsgegevens als verwerker (inkomend)

Indien persoonsgegevens door een derde partij aan een groepsonderneming van Arbonia worden doorgegeven, moet ervoor worden gezorgd dat de persoonsgegevens (i) voor het beoogde doel kunnen worden gebruikt, (ii) op legitieme gronden worden verzameld (het verdient aanbeveling een schriftelijke bevestiging te verkrijgen) en (iii) er een overeenkomst voor de verwerking van de gegevens bestaat die voldoet aan artikel 28 van de AVG.

7.3 Grensoverschrijdende overdracht van persoonsgegevens

In het geval van grensoverschrijdende overdracht van persoonsgegevens moet worden voldaan aan de respectieve nationale vereisten voor de bekendmaking van persoonsgegevens in het buitenland. In het kader van de AVG kan doorgifte van persoonsgegevens plaatsvinden binnen de EU, de EER of naar een land waarvan de Europese Commissie heeft vastgesteld dat het voldoende waarborgen biedt voor een passend niveau van gegevensbescherming. Voor een dergelijke gegevensdoorgifte is geen speciale

toestemming nodig. De Europese Commissie heeft Zwitserland geclassificeerd als een land dat adequate bescherming biedt (zie de huidige lijst van landen: < https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en >.

Een overdracht van persoonsgegevens naar een derde land is alleen toegestaan als er verdere adequate waarborgen zijn. Dit betekent dat als de ontvanger kan aantonen dat hij/zij een gegevensbeschermingsnorm handhaaft die in overeenstemming is met deze richtlijn inzake gegevensbescherming (bijvoorbeeld i) er bindende bedrijfsvoorschriften bestaan, ii) er met de dienstverlener en andere onderaannemers EU-standaardcontractbepalingen voor de verwerking in derde landen zijn gesloten[3], iii) er door de toezichthoudende autoriteit goedgekeurde gedragsregels bestaan, iv) wanneer de dienstverlener deelneemt aan een door de EU geaccrediteerde certificeringsregeling, om een passend niveau van gegevensbescherming te bereiken, of v) met individuele overeenkomsten tussen de voor verwerkingsverantwoordelijke en de verwerker met toestemming van de bevoegde toezichthoudende autoriteit) en met informatie aan de betrokkene. Deze verplichting is niet van toepassing als de overdracht is gebaseerd op een wettelijke verplichting. Voor een dergelijke overdracht is de goedkeuring van de coördinator voor gegevensbescherming of de functionaris voor gegevensbescherming vereist.

Indien persoonsgegevens binnen Arbonia worden overgedragen, is de groepsonderneming die de persoonsgegevens invoert, verplicht om mee te werken aan alle verzoeken van de bevoegde toezichthoudende autoriteit in het land waar de exporterende groepsonderneming haar statutaire zetel heeft, en om te voldoen aan alle opmerkingen van de respectieve toezichthoudende autoriteit met betrekking tot de verwerking van de overgedragen persoonsgegevens.

7.4 Behandeling van een verzoek om informatie door een betrokkene

De betrokkenen hebben het recht om een formeel verzoek om informatie over de persoonsgegevens van Arbonia in te dienen en kunnen om het volgende verzoeken:

Recht op toegang tot informatie over:

- het verwerkingsdoel;
- de categorieën van verwerkte persoonsgegevens;
- de ontvangers of categorieën ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name aan ontvangers in derde landen of aan internationale organisaties;
- indien mogelijk, de geplande duur van de opslag van de persoonsgegevens of, indien dit niet mogelijk is, de criteria voor het bepalen van deze duur;

[3] Zie het besluit van de Commissie van 5 februari 2010 betreffende modelcontractbepalingen voor de doorgifte van persoonsgegevens aan in derde landen gevestigde verwerkers krachtens Richtlijn 95/46/EG van het Europees Parlement en de Raad, < https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087 >

- het bestaan van een recht van rectificatie of verwijdering van de hen betreffende persoonsgegevens of van een recht van verzet tegen of beperking van de verwerking door de verwerkingsverantwoordelijke;
- het bestaan van een recht van beroep bij een toezichthoudende autoriteit;
- alle beschikbare informatie over de oorsprong van de gegevens, indien de persoonsgegevens niet bij de betrokkene worden verzameld;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering
- Wanneer persoonsgegevens worden doorgegeven aan een derde land of aan een internationale organisatie, heeft de betrokkene het recht te worden geïnformeerd over de passende waarborgen.

Recht op correctie:

- De betrokkene heeft het recht om van de verwerkingsverantwoordelijke onverwijld de rectificatie te verkrijgen van onjuiste persoonsgegevens die op hem of haar betrekking hebben. Gelet op de doeleinden van de verwerking heeft de betrokkene het recht om de vervollediging van onvolledige persoonsgegevens te verkrijgen, onder meer door middel van een aanvullende verklaring.

Recht op verwijdering („Recht op vergeten te worden"):

- De betrokkene heeft het recht de verwerkingsverantwoordelijke te verzoeken de hem of haar betreffende persoonsgegevens onverwijld te verwijderen en de verwerkingsverantwoordelijke is verplicht de persoonsgegevens onverwijld te verwijderen indien een van de volgende redenen van toepassing is:
    1. De persoonsgegevens zijn niet langer noodzakelijk voor de doeleinden waarvoor zij worden verzameld of anderszins worden verwerkt;
    2. De betrokkene trekt de toestemming waarop de verwerking was gebaseerd in overeenkomstig artikel 6, lid 1(a), van de AVG of artikel 9, lid 2(a), van de AVG en er is geen andere rechtsgrond voor de verwerking;
    3. De betrokkene maakt bezwaar tegen de verwerking op grond van artikel 21, lid 1, van de AVG en er zijn geen dwingende legitieme redenen voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking op grond van artikel 21, lid 2, van de AVG;
    4. De persoonsgegevens zijn onrechtmatig verwerkt;
    5. De verwijdering van persoonsgegevens is noodzakelijk om te voldoen aan een wettelijke verplichting krachtens de wetgeving van de lidstaten waaraan de verwerkingsverantwoordelijke is onderworpen;
    6. De persoonsgegevens zijn verzameld in verband met de diensten van de informatiemaatschappij die worden aangeboden overeenkomstig artikel 8, lid 1, van de AVG.

Recht om de verwerking te beperken:

- De betrokkene heeft het recht om van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen indien aan een van de volgende voorwaarden is voldaan:

- indien de juistheid van de persoonsgegevens door de betrokkene wordt betwist, gedurende een periode die de verwerkingsverantwoordelijke in staat stelt de juistheid van de persoonsgegevens te verifiëren:
- indien de verwerking onrechtmatig is en de betrokkene weigert de persoonsgegevens te laten verwijderen en in plaats daarvan verzoekt om beperking van het gebruik van de persoonsgegevens;
- wanneer de verwerkingsverantwoordelijke de persoonsgegevens niet langer nodig heeft voor de doeleinden van de verwerking, maar de betrokkene deze nodig heeft om zijn rechten uit te oefenen of te verdedigen,
- wanneer de betrokkene overeenkomstig artikel 21, lid 1, bezwaar tegen de verwerking heeft gemaakt, in afwachting van de vaststelling of de gerechtvaardigde redenen van de verwerkingsverantwoordelijke zwaarder wegen dan die van de betrokkene.

De betrokkene dient te worden verzocht zijn of haar verzoek schriftelijk in te dienen, hetzij per e-mail, hetzij per post, gericht aan de bevoegde plaatselijke functionaris voor gegevensbescherming. Informatie wordt door de plaatselijke functionaris voor gegevensbescherming onverwijld, maar in ieder geval binnen een maand na ontvangst van het verzoek, aan de betrokkene ter beschikking gesteld. Deze periode kan met nog eens twee maanden worden verlengd als dat nodig is gezien de complexiteit en het aantal aanvragen. De gegevensbeschermingscoördinator of de gegevensbeschermingsfunctionaris van de verwerkingsverantwoordelijke stelt de betrokkene binnen een maand na ontvangst van het verzoek in kennis van een eventuele verlenging van de termijn, met opgave van de redenen voor de vertraging. De betrokkene mag geen kosten maken voor het opvragen van informatie over de informatie die een groepsonderneming van Arbonia over hem of haar in haar bezit heeft, tenzij verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name als gevolg van een herhaaldelijke standpuntbepaling. Vragen van een betrokkene over verschillende groepsondernemingen van Arbonia moeten worden doorgestuurd naar Corporate IT voor coördinatie en een antwoord.

7.5 Uitvoering van een effectbeoordeling inzake gegevensbescherming

Wanneer een voorgestelde nieuwe vorm van verwerking van persoonsgegevens, met name wanneer nieuwe technologieën worden gebruikt, gezien de aard, de omvang, de omstandigheden en de doeleinden van de verwerking waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen inhoudt, wordt voorafgaand aan de verwerking een beoordeling van het effect van de voorgestelde verwerkingshandelingen op de bescherming van de persoonsgegevens uitgevoerd.

Alvorens nieuwe verwerkingen uit te voeren, moeten de daaruit voortvloeiende risico's voor de persoonlijkheid en de grondrechten van de betrokkene derhalve worden beoordeeld. In het geval van nieuwe IT-toepassingen moet hiermee rekening worden gehouden bij het goedkeuringsproces. Indien uit een eerste beoordeling blijkt dat een geplande nieuwe vorm

van verwerking van persoonsgegevens waarschijnlijk een groot risico voor de betrokkene inhoudt, moet een effectbeoordeling voor de gegevensbescherming worden uitgevoerd.

Vragen over de noodzaak van of tijdens de uitvoering van een effectbeoordeling voor de gegevensbescherming moeten worden gericht aan de plaatselijke coördinator voor gegevensbescherming of de plaatselijke functionaris voor gegevensbescherming. Nadat de effectbeoordeling voor gegevensbescherming is uitgevoerd, moet de plaatselijke coördinator voor gegevensbescherming of de plaatselijke functionaris voor gegevensbescherming op de hoogte worden gesteld van deze effectbeoordeling en moet hem of haar worden gevraagd zijn advies uit te brengen.

Indien uit een effectbeoordeling inzake gegevensbescherming blijkt dat de verwerking een groot risico voor de betrokkene met zich meebrengt en er geen maatregelen worden genomen om het risico te beperken, moet de toezichthoudende autoriteit worden geraadpleegd voordat de nieuwe verwerkingen worden uitgevoerd.

8 BEVEILIGING VAN PERSOONSGEGEVENS

Persoonsgegevens moeten worden beschermd tegen ongeoorloofde toegang en onwettige verwerking of openbaarmaking en tegen onopzettelijk verlies, wijziging of vernietiging. Dit geldt ongeacht of de persoonsgegevens elektronisch of op papier worden verwerkt.

Verantwoordelijken en verwerkers moeten passende technische en organisatorische maatregelen treffen om gegevens te beschermen tegen onrechtmatige verwerking. Deze maatregelen moeten gebaseerd zijn op (i) beste praktijken, (ii) de risico's van de verwerking, en (iii) de noodzaak om persoonsgegevens te beschermen (zoals bepaald door het informatieclassificatieproces), met inbegrip van onder meer de vraag hoe passend in elk geval:

(a) de pseudonimisering en versleuteling van persoonsgegevens;

(b) het vermogen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de systemen en diensten met betrekking tot de verwerking op lange termijn te waarborgen;

(c) de mogelijkheid om de beschikbaarheid van en de toegang tot persoonsgegevens snel te herstellen in geval van een fysiek of technisch incident;

(d) een procedure voor de regelmatige herziening, beoordeling en evaluatie van de doeltreffendheid van de technische en organisatorische maatregelen om de veiligheid van de verwerking te waarborgen.

De technische en organisatorische maatregelen voor de bescherming van persoonsgegevens maken deel uit van het interne informatiebeveiligingsbeheer en moeten voortdurend worden aangepast aan de technische ontwikkelingen en organisatorische veranderingen.

De veiligheidsprocedures kunnen ten minste omvatten

- Toegangscontrole: Elke onbekende die in toegangscontrolegebieden wordt aangetroffen, moet worden gemeld.

- Veilige vergrendelbare laden of archiefkasten: Bureaus en kasten moeten op slot worden gehouden als ze vertrouwelijke informatie van welke aard dan ook bevatten. Persoonsgegevens zijn altijd vertrouwelijke informatie. Beschäftigte sollten sicherstellen, dass Papier und Ausdrucke mit personenbezogenen Daten nicht allgemein sichtbar hinterlassen werden, wie etwa in einem Drucker. Wanneer geautoriseerde persoonsgegevens worden opgeslagen op een verwisselbaar medium (zoals een cd, memory stick of dvd), moeten deze veilig worden opgeborgen wanneer ze niet worden gebruikt.
- verwijderingsmethoden: Documenten op papier moeten worden versnipperd en veilig worden verwijderd wanneer ze niet meer nodig zijn. Dit geldt ook voor persoonsgegevens die meestal elektronisch worden opgeslagen, maar die wel zijn uitgeprint.

- Gegevens opgeslagen in elektronische vorm: Persoonsgegevens moeten worden beschermd met wachtwoorden volgens het huidige wachtwoordbeleid en mogen nooit worden uitgewisseld tussen medewerkers. Indien een elektronisch formulier van toepassing is, moeten persoonsgegevens worden opgeslagen en opgehaald op IT-serversystemen en in gestructureerde informatietechnologische toepassingen, in plaats van in onversleutelde vorm op lokale computers.

- Persoonsgegevens die in elektronische vorm worden verzameld en door de betrokkene worden verstrekt: De identiteit van de betrokkene moet worden geverifieerd, bij voorkeur door middel van een dubbele opt-in procedure (d.w.z. een tweede e-mail om het verstrekte e-mailadres te valideren). Als de toegang tot een website of app beperkt is tot geregistreerde gebruikers (d.w.z. gebruikersaccount), moet de identificatie en authenticatie van de betrokken persoon een veiligheidsbescherming bieden die evenredig is met de inhoud in kwestie tijdens de toegang.

- Wees voorzichtig met het delen van persoonsgegevens: Persoonsgegevens mogen nooit informeel worden gedeeld. Het principe van "noodzakelijke informatie" is van toepassing. Een concept van uitsplitsing en scheiding per bedrijfsproces en de implementatie van rollen en verantwoordelijkheden is verplicht. Persoonsgegevens moeten in elektronische vorm worden versleuteld, voordat ze worden verzonden. De

IT-manager kan uitleggen hoe persoonlijke informatie naar geautoriseerde externe contactpersonen wordt gestuurd.

- Verkrijg instructies: Als u vragen of problemen heeft met betrekking tot een aspect van gegevensbescherming of verplichtingen in het kader van deze richtlijn inzake gegevensbescherming, moet u advies inwinnen bij uw directe supervisor, de relevante lokale functionaris voor gegevensbescherming of Legal & Compliance.

De AVG vereist dat er in een zo vroeg mogelijk stadium rekening wordt gehouden met de privacy. Privacy door middel van technologieontwerp vereist dat organisaties rekening houden met privacy in de vroege stadia van technologieontwerp en bij de ontwikkeling van nieuwe producten, processen of diensten die de verwerking van persoonsgegevens met zich meebrengen. Privacy betekent standaard dat wanneer een systeem of dienst de beslissing van een individu inhoudt om hoeveel persoonlijke informatie met anderen te delen, de standaardinstellingen de grootste bescherming van de privacy moeten bieden. Daarom wordt elke nieuwe IT-toepassing onderworpen aan een intern goedkeuringsproces, waarbij deze nieuwe IT-toepassing in het kader van de evaluatie ook vanuit het oogpunt van gegevensbescherming moet worden geëvalueerd.

9 MELDING VAN INCIDENTEN OP HET GEBIED VAN GEGEVENSBEVEILIGING

Veel van de geldende regels voor gegevensbescherming vereisen dat incidenten op het gebied van gegevensbescherming rechtstreeks aan de wetgever worden gemeld. Het is daarom vereist dat alle incidenten op het gebied van gegevensbeveiliging onmiddellijk worden gemeld aan de verantwoordelijke coördinator of functionaris voor gegevensbescherming, ongeacht of het gaat om een lokaal systeem of een bedrijfssysteem, in overeenstemming met de richtlijn van Arbonia inzake gegevensbeveiliging ("Arbonia Data Breach Policy"). Indien de IT-afdeling incidenten of risico's op het gebied van gegevensbeveiliging vaststelt, moeten deze worden gemeld overeenkomstig de Data Breach Notification-richtlijn.

Het doel is om te voldoen aan de verplichtingen met betrekking tot de melding van een inbreuk op de toepasselijke gegevensbeschermingswetgeving (bijvoorbeeld in het kader van de AVG uiterlijk binnen 72 uur na kennisname daarvan).

In een dergelijk geval moet de nadruk worden gelegd op het naleven van de respectieve termijnen voor het melden van inbreuken op de gegevensbescherming en het nemen van onmiddellijke maatregelen om incidenten te onderzoeken en vast te stellen of er daadwerkelijk sprake is van een inbreuk in verband met de persoonsgegevens. Corporate IT moet een interne lijst van veiligheidsinbreuken bij Arbonia bijhouden, zodat de meldingsverplichtingen uit hoofde van het nationale recht kunnen worden nageleefd en ervoor kan worden gezorgd dat de respectieve vertegenwoordigingsregels worden toegepast, zodat inbreuken te allen tijde kunnen worden gemeld. Alvorens een melding te

doen aan een nationale autoriteit, moet Corporate IT of de afdeling Legal and Compliance van de Groep op de hoogte worden gebracht.

Alle andere instructies van Corporate IT en lokale IT-afdelingen moeten strikt worden opgevolgd.

10 GEVOLGEN VAN NIET-NALEVING

De naleving van deze gegevensbeschermingsrichtlijn is van het grootste belang voor Arbonia en de publieke perceptie van Arbonia. Ongepaste verwerking van persoonsgegevens of andere schendingen van de wetgeving inzake gegevensbescherming kunnen in veel landen ook onderworpen zijn aan een strafrechtelijk bevel en leiden tot schadevorderingen. Binnen Arbonia kan een overtreding van bepalingen uiteengezet in deze richtlijn inzake gegevensbescherming leiden tot sancties op grond van de wet en/of de relevante (arbeids)overeenkomst.

11 AFWIJKINGEN

Afwijkingen van de bepalingen van deze richtlijn en de addenda zijn alleen toegestaan na overleg met het hoofd van Legal & Compliance.

12 INFORMATIE

Informatie in verband met de richtlijn inzake gegevensbescherming kan worden verkregen bij het hoofd van Legal & Compliance.

13 INWERKINGTREDING

Deze richtlijn treedt in werking op 17 juni 2020 en vervangt de richtlijn betreffende de verwerking van gegevens (gegevensbeschermingsrichtlijn) van 5 december 2013.

Arbon, 16 juni 2020

Arbonia AG

Alexander von Witzleben
Voorzitter van de Raad van Bestuur en CEO

Andrea Wickart
Hoofd van Legal & Compliance / algemeen secretaris

ARBONIA

Aanvullingen op deze richtlijn inzake gegevensbescherming van Arbonia:

De volgende aanvullingen in hun huidige versie concretiseren deze richtlijn inzake gegevensbescherming:

- Richtlijn over verzoeken van betrokkenen en over het wissen van gegevens
- Richtlijn over inbreuken op de gegevensbescherming
- Richtlijn inzake gegevensbescherming voor werknemers

Dit document is geldig zonder handtekening.