Bijlage 9: Verwerkersovereenkomst Generieke RAS

Tussen

ProRail B.V.
als Verantwoordelijke

en

[Verwerker]
als Verwerker

Inhoud

DE ONDERGETEKENDEN:

1. De besloten vennootschap met beperkte aansprakelijkheid ProRail B.V., statutair gevestigd te Utrecht, kantoorhoudende op het adres Moreelsepark 3, 3511 EP Utrecht, ingeschreven in het handelsregister onder nummer 30.124.359, in deze rechtsgeldig vertegenwoordigd door [de heer/mevrouw naam], [functie], en [de heer/mevrouw naam], [functie], hierna te noemen: '**Verantwoordelijke**',

en

2. [heer/mevrouw naam], statutair gevestigd te [plaats], kantoorhoudende op het adres [adres], [postcode/plaats], ingeschreven in het handelsregister onder nummer [nummer], in deze rechtsgeldig vertegenwoordigd door [heer/mevrouw naam], [functie], hierna te noemen: '**Verwerker**';

Verantwoordelijke en Verwerker gezamenlijk ook te noemen als '**Partijen**' en ieder afzonderlijk als '**Partij**'.

OVERWEGENDE DAT:

A. Partijen op [datum] een overeenkomst 'Generieke RAS' zijn aangegaan met betrekking tot het leveren van een Systeem voor digitale toegang tot de relevante onderdelen van het ProRail-netwerk (hierna te noemen: '**Hoofdovereenkomst**');

B. De uitvoering van deze Hoofdovereenkomst met zich meebrengt dat conform instructie van Verantwoordelijke Persoonsgegevens door Verwerker worden verwerkt;

C. De Verwerker deze Persoonsgegevens niet voor eigen doeleinden mag verwerken;

D. Partijen in deze Verwerkersovereenkomst de afspraken over de Verwerking van Persoonsgegevens in het kader van de overeengekomen diensten wensen vast te leggen.

Artikel 1 Begrippen

In deze Overeenkomst wordt onder de volgende begrippen verstaan (de begrippen kunnen zonder verlies van betekenis in het enkelvoud of in het meervoud worden gebruikt of worden vervoegd):

1. Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

2. Datalek: een inbreuk op de beveiliging, in de zin van de Geldende Privacy-wetgeving.

3. Geldende Privacywetgeving: de toepasselijke privacywetgeving, waaronder de Algemene verordening gegevensbescherming, de Uitvoeringswet Algemene verordening gegevensbescherming en overige van toepassing zijnde wet- en regelgeving.

4. Hoofdovereenkomst: de overeenkomst 'Generieke RAS' tussen Partijen van [datum].

5. Personeel: de door een Partij voor de uitvoering van de Hoofdovereenkomst in te schakelen werknemers, uitzendkrachten en dergelijke, welke onder diens eigen

verantwoordelijkheid zullen werken.

6. Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon als bedoeld in Geldende Privacywetgeving.

7. Wet publiekrechtelijke omvorming ProRail (wetsvoorstel): Wet tot wijziging van de Spoorwegwet en enige andere wetten in verband met de omvorming van Verantwoordelijke tot een publiekrechtelijke zelfstandig bestuursorgaan.

8. Verantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt.

9. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verantwoordelijke Persoonsgegevens verwerkt.

10. Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

11. Verwerking van Persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens (al dan niet geautomatiseerd), waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Artikel 2 Doel van de verwerking

1. Verwerker zal in het kader van de uitvoering van de in de Hoofdovereenkomst overeengekomen werkzaamheden ten behoeve van Verantwoordelijke Persoonsgegevens verwerken conform schriftelijke instructies van Verantwoordelijke.
   De werkzaamheden, het doel van de verwerking, de te verwerken Persoonsgegevens en de categorieën Betrokkenen worden beschreven in **bijlagen 1 en 2**.

Artikel 3 Totstandkoming, duur en einde van de Verwerkersovereenkomst

1. De Verwerkersovereenkomst treedt gelijktijdig met de Hoofdovereenkomst in werking, zo nodig met terugwerkende kracht.

2. De Verwerkersovereenkomst zal van kracht zijn voor de duur van de Hoofdovereenkomst. De Verwerkersovereenkomst eindigt van rechtswege op het moment dat de Hoofdovereenkomst eindigt en Verwerker iedere verwerking, die op verzoek van Verantwoordelijke plaatsvond, heeft gestaakt.

3. Geen van beide Partijen kan de Verwerkersovereenkomst tussentijds opzeggen behalve in gevallen zoals bedoeld in artikel 4 lid 1 van deze Verwerkersovereenkomst en onderhavig lid. Verantwoordelijke is bevoegd om de Verwerkersovereenkomst en de Hoofdovereenkomst (gedeeltelijk) buitengerechtelijk te ontbinden indien sprake is van een Datalek bij Verwerker dan wel diens sub-verwerkers waarbij Persoonsgegevens behorende tot de Hoofdovereenkomst zijn betrokken, tenzij het datalek gezien haar bijzondere aard of geringe

betekenis, deze ontbinding met haar gevolgen niet rechtvaardigt.

4. Na afloop van de Hoofdovereenkomst dienen alle Persoonsgegevens, kopieën en bewerkingen daarvan, onmiddellijk op eerste verzoek van Verantwoordelijke in een door Verantwoordelijke gewenste vorm te worden geretourneerd c.q. verstrekt aan Verantwoordelijke, dan wel aan een opvolgende verwerker dan wel te worden vernietigd op een door Verantwoordelijke aangegeven wijze, een en ander naar keuze van Verantwoordelijke. Op het moment dat deze Verwerkersovereenkomst eindigt, zal Verwerker bovendien al zijn medewerking verlenen ter zake van de overdracht van de werkzaamheden inzake de Verwerking van de Persoonsgegevens aan Verantwoordelijke of een opvolgende verwerker en wel op zodanige wijze dat vanaf het moment dat de overdracht plaatsvindt de continuïteit van de dienstverlening maximaal gewaarborgd blijft, althans niet door handelen of nalaten van Verwerker wordt belemmerd. De kosten gemoeid met deze inspanningen van Verwerker, komen voor rekening van Verantwoordelijke voor zover deze kosten niet inbegrepen zijn in de overeengekomen prijzen en vergoedingen van Verwerker voortvloeiende uit de uitvoering van de Hoofdovereenkomst.

5. Verwerker zal op eerste verzoek van Verantwoordelijke schriftelijk verklaren dat de Persoonsgegevens zijn vernietigd.

Artikel 4 Verplichtingen van Verwerker

1. Verwerker verwerkt Persoonsgegevens slechts in opdracht van Verantwoordelijke en volgt dienaangaande alle schriftelijke instructies van Verantwoordelijke op, behoudens afwijkende wettelijke verplichtingen. In dat geval zal Verwerker onverwijld Verantwoordelijke schriftelijk informeren over deze afwijkende wettelijke verplichting, in welk geval Verantwoordelijke de gegevensdoorgifte mag opschorten en/of de Verwerkersovereenkomst en/of de Hoofdovereenkomst mag opzeggen.
   Onder schriftelijk wordt verstaan per e-mail of brief.

2. Verwerker heeft geen zeggenschap over het doel en de middelen van de verwerking van de door Verantwoordelijke aan hem verstrekte Persoonsgegevens.

3. Niets in deze overeenkomst is bedoeld om op enigerlei wijze de zeggenschap ten aanzien van de Persoonsgegevens die aan Verwerker worden verstrekt aan Verwerker over te dragen.

4. Verwerker zal de Persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de Geldende Privacywetgeving en deze Verwerkersovereenkomst verwerken.
   De verstrekte Persoonsgegevens zullen door Verwerker nimmer voor eigen doeleinden en/of die van derden worden verwerkt.

5. De verplichtingen van de Verwerker die uit deze Verwerkersovereenkomst voortvloeien, gelden ook voor degenen die Persoonsgegevens verwerken onder het gezag van Verwerker, waaronder begrepen maar niet beperkt tot diens Personeel, in de ruimste zin van het woord.

6. Verwerker mag uitsluitend na voorafgaande specifieke schriftelijke toestemming van Verantwoordelijke een derde (sub-verwerker) inschakelen bij de uitvoering van deze Verwerkersovereenkomst, onder de voorwaarden dat in de subverwerkersovereenkomst gelijke of strengere voorwaarden aan verwerking van Persoonsgegevens zoals aangegeven in deze Verwerkersovereenkomst zijn opgenomen. Verantwoordelijke wordt in staat gesteld om toe te zien op naleving. Verwerker verstrekt pas Persoonsgegevens aan sub-Verwerker, nadat er een sub-Verwerkersovereenkomst met de sub-Verwerker is overeengekomen.

7. Verwerker zal te allen tijde op eerste verzoek van Verantwoordelijke alle vragen van Verantwoordelijke betreffende de door Verwerker uitgevoerde verwerking van de doorgegeven Persoonsgegevens zo spoedig mogelijk naar behoren beantwoorden, en het advies van de toezichthoudende autoriteit volgen bij de verwerking van de doorgegeven Persoonsgegevens.

8. Verwerker garandeert dat zijn Personeel of Personeel van onderaannemers of hulppersonen, op een 'need-to-know' basis toegang tot de gegevens zullen hebben, en zich zullen onthouden van kopiëren, doorgeven of overdragen, uittreksels maken of verspreiden van Persoonsgegevens op welke wijze dan ook aan een andere partij, inclusief ander Personeel van Verwerker die niet betrokken zijn bij de uitvoering van de Hoofdovereenkomst tussen partijen of de diensten.

9. Verwerker verleent Verantwoordelijke te allen tijde volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de Geldende Privacywetgeving, zoals, maar niet beperkt tot, een verzoek van Betrokkene om inzage, verbetering, aanvulling, verwijdering, overdracht of afscherming van Persoonsgegevens en het uitvoeren van een aangetekend verzet.

10. Het is Verwerker niet toegestaan Persoonsgegevens aan anderen dan Verantwoordelijke te verstrekken, tenzij op schriftelijk verzoek van Verantwoordelijke, of met diens schriftelijke toestemming. Verwerker is verplicht schriftelijk te bevestigen dat een dergelijke verstrekking heeft plaatsgevonden, waarbij exact de verstrekte Persoonsgegevens, de Betrokkenen(n), de ontvanger(s), en het moment van verstrekking worden beschreven. Verantwoordelijke bewaart de afwijkende verstrekking gedurende drie jaren.

11. Indien Verwerker op grond van een wettelijke verplichting Persoonsgegevens dient te verstrekken, verifieert Verwerker de grondslag van het verzoek en de identiteit van de verzoeker en overlegt hij onmiddellijk na ontvangst van gemeld verzoek met Verantwoordelijke of en op welke wijze aan het verzoek wordt voldaan.

12. Verwerker informeert Verantwoordelijke zo spoedig mogelijk, maar uiterlijk binnen 24 uur na constatering van een Datalek. Hierna houdt Verwerker Verantwoordelijke op de hoogte van nieuwe ontwikkelingen rond het Datalek, en van de maatregelen die Verwerker treft om de gevolgen van het Datalek te beperken en herhaling te voorkomen. Tevens verleent Verwerker Verantwoordelijke volledige medewerking aan het voldoen aan de ter zake geldende meldingsplichten aan de Autoriteit Persoonsgegevens en de Betrokkenen. Verwerker verstrekt daarbij de informatie en verleent de medewerking zoals vermeld in **bijlage 3.**

Artikel 5 Beveiliging

1. Verwerker zal alle noodzakelijke technische- en organisatorische beveiligingsmaatregelen implementeren benodigd om de bescherming van de Persoonsgegevens optimaal te garanderen en om te voldoen aan ter zake Geldende Privacywetgeving zoals maar niet beperkt tot en voor zover passend:

   a) de pseudonimisering en versleuteling van Persoonsgegevens;

   b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

   c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de

toegang tot de Persoonsgegevens tijdig te herstellen;

d) een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

2. Zie **bijlage 4** voor een specificatie van het vereiste niveau van beveiliging per de datum van ondertekening van deze Verwerkersovereenkomst door Partijen. Deze maatregelen zullen, met inachtneming van de stand der techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het Verwerken van de Persoonsgegevens en de aard daarvan, meebrengen. Verwerker zal redelijke instructies van Verantwoordelijke met het oog op beveiligingsmaatregelen onverwijld opvolgen.

3. Verwerker verwerkt geen Persoonsgegevens buiten een lidstaat van de Europese Economische Ruimte (EER), tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Verantwoordelijke.

Artikel 6 Geheimhouding

1. Verwerker is gehouden tot geheimhouding van alle Persoonsgegevens en informatie die hij als uitvloeisel van deze Verwerkersovereenkomst verwerkt, behoudens indien Verwerker op grond van een wettelijke verplichting verplicht is om de Persoonsgegevens aan derde(n) te verstrekken. Indien en voor zover Verantwoordelijke daarom uitdrukkelijk schriftelijk verzoekt, zal Verwerker ten aanzien van de daarbij aangeduide gegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van de betrokken Persoonsgegevens of informatie zodra de noodzaak voor Verwerker om daarvan nog langer kennis te nemen, is komen te vervallen.

2. Verwerker zal haar overeenkomsten met haar Personeel, onderaannemers en ieder ander die handelt onder de verantwoordelijkheid van Verwerker, bedingen dat door die personen op overeenkomstige wijze als in dit lid 1 is bepaald, geheimhouding zal worden betracht ten aanzien van alle Persoonsgegevens en informatie die zij in het kader van hun werkzaamheden voor Verwerker verwerken. Verwerker staat er jegens Verantwoordelijke voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.

3. Na afloop van de Hoofdovereenkomst en deze Verwerkersovereenkomst blijft dit artikel en de hierin besproken geheimhouding van kracht.

Artikel 7 Toezicht

1. Verantwoordelijke kan op elk door haar gewenst moment de Verwerkingen en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen, inclusief datalekprotocollen van Verwerker dan wel die van door Verwerker ingeschakelde derden, (laten) controleren.

2. Verwerker verbindt zich om binnen een door Verantwoordelijke te bepalen termijn aan het betrokken Personeel van Verantwoordelijke of door Verantwoordelijke ingeschakelde derden alle verlangde informatie te verstrekken met inachtneming van redelijkheid en billijkheid.

Verantwoordelijke en diens Personeel en ingeschakelde derden zullen vertrouwelijk met deze informatie omgaan.

3. Verwerker staat ervoor in de door de Verantwoordelijke of door Verantwoordelijke ingeschakelde derde aangegeven aanbevelingen ter verbetering binnen de daartoe door Verantwoordelijke te bepalen termijn uit te voeren. De kosten hiervan worden door Verwerker gedragen voor zover de aanbevelingen zijn gebaseerd op geldende wet- en regelgeving. Overige kosten voor opvolging door Verwerker zijn voor Verantwoordelijke.

4. De kosten van het onderzoek komen voor rekening van Verantwoordelijke, tenzij uit de controle blijkt dat Verwerker is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst en/of de Hoofdovereenkomst.

Artikel 8 Aansprakelijkheid

1. Verwerker is aansprakelijk voor alle aan Verwerker toe te rekenen schade voortvloeiende uit of verband houdend met het niet of niet behoorlijk nakomen van deze Verwerkersovereenkomst dan wel handelen in strijd met de Geldende Privacywetgeving, onverminderd de aanspraken op grond van andere wettelijke regels.

2. Verwerker vrijwaart Verantwoordelijke tegen aanspraken van derden, waaronder Betrokkenen, in verband met het toerekenbaar tekortschieten van Verwerker in de nakoming van de Verwerkersovereenkomst of overtreding door Verwerker van de Geldende Privacywetgeving en zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen kosten van juridische bijstand) en schade (waaronder boetes) van Verantwoordelijke vergoeden.

3. Partijen verklaren uitdrukkelijk dat beperking van de aansprakelijkheid op grond van de Hoofdovereenkomst en/of de inkoopvoorwaarden behorende tot de Hoofdovereenkomst niet van toepassing is op onderhavige Verwerkersovereenkomst.

4. Bij overtreding van het in artikel 5 bepaalde, zal Verwerker aan Verantwoordelijke een onmiddellijk opeisbare boete betalen van € 5.000,00 (zegge: vijfduizend euro) per overtreding en € 500,00 (zegge: vijfhonderd euro) per dag dat de overtreding voortduurt met een maximum van € 25.000,00 (zegge: vijfentwintigduizend euro). Deze boete laat onverlet het recht van Verantwoordelijke op nakoming van het bepaalde in artikel 5 van deze Verwerkersovereenkomst en treedt niet in de plaats van het recht van Verantwoordelijke op schadevergoeding.

Artikel 9 Eigendomsrechten

1. Alle externe gegevensdragers, zoals, doch niet beperkt tot CD’s , DVD's, USB-sticks, harde schijven of papier, voorzien van (Persoons)-gegevens, die zijn verstrekt door Verantwoordelijke worden geacht volle eigendom van Verantwoordelijke te zijn en te blijven. Verwerker zal nimmer enig recht claimen ten aanzien van de betrokken gegevens noch gerechtigd zijn tot enige vorm van exploitatie anders dan voorzien in deze Verwerkersovereenkomst.

Artikel 10 Overige bepalingen

1. De volgende bijlagen maken integraal onderdeel uit van deze Verwerkersovereenkomst:

- bijlage 1: werkzaamheden en doel van de werkzaamheden;
- bijlage 2: beschrijving van Persoonsgegevens & categorieën van Betrokkenen;
- bijlage 3: maatregelen in verband met de meldplicht datalekken;
- bijlage 4: passende technische- en organisatorische maatregelen.

2. In aanvulling op het bovenstaande dient Opdrachtnemer voor persoonsgegevens te voldoen aan de verplichtingen omtrent cybersecurity zoals opgenomen in het PvE.

3. De gehele of gedeeltelijke ongeldigheid van een of meer bepalingen van deze Verwerkersovereenkomst, brengt niet de nietigheid of vernietigbaarheid van de gehele Verwerkersovereenkomst met zich mee. Voor zover de bedoelde ongeldigheid betrekking heeft op een wezenlijk onderdeel van de relatie tussen Partijen, zullen Partijen in overleg vaststellen welke wijzigingen in de Verwerkersovereenkomst noodzakelijk zijn om die ongeldigheid te herstellen, waarbij zoveel mogelijk aansluiting zal worden gezocht bij de bedoeling van Partijen zoals die uit de Verwerkersovereenkomst blijkt.

4. Deze Verwerkersovereenkomst kan, met uitzondering van hetgeen bepaald is in artikel 4 eerste lid, slechts worden gewijzigd door middel van een schriftelijk stuk waarin uitdrukkelijk staat vermeld dat het stuk bedoelt een dergelijke wijziging aan te brengen en dat door ter zake bevoegde vertegenwoordigers van Partijen is ondertekend.

5. Deze Verwerkersovereenkomst vormt een aanvulling op de Hoofdovereenkomst. Bij strijdigheid tussen bepalingen uit deze Verwerkersovereenkomst en de Hoofdovereenkomst betreffende de verwerking van Persoonsgegevens prevaleren de bepalingen uit deze Verwerkersovereenkomst.

Artikel 11 Geschillen, toepasselijk recht en bevoegde rechter

1. Op deze Verwerkersovereenkomst en op alle geschillen die daaruit mochten voortvloeien of daarmee mochten samenhangen, is Nederlands recht van toepassing.

2. Ieder geschil tussen Partijen ter zake van deze Verwerkersovereenkomst zal bij uitsluiting worden voorgelegd aan de daartoe bevoegde rechter te Utrecht.

ALDUS IN TWEEVOUD OPGEMAAKT EN ONDERTEKEND,

te ……	te …….
d.d. …….	d.d. ….……
Verantwoordelijke	Verwerker
[naam] [functie]	[naam] [functie]
[naam] [functie]	

Bijlage 1 Werkzaamheden in de Hoofdovereenkomst

Verantwoordelijke heeft aan Verwerker een opdracht gegeven tot

- Levering van een Dienst voor digitale toegang;
- Hosting en technisch onderhoud van de Dienst;
- Uitvoeren van servicedesk- en supportwerkzaamheden.

De werkzaamheden die onder deze Verwerkersovereenkomst vallen, betreffen

- Verwerking van gebruikersgegevens (voor-/achternaam, e-mail, telefoonnummer en bedrijf) voor de toepassing van de Dienst;
- Logregistratie voor beveiliging en auditing;
- Opslag van configuratie- en gebruiksgegevens;
- Incidentregistratie en probleemoplossing.

Het doel van deze werkzaamheden die onder deze Verwerkersovereenkomst vallen, is

- Het kunnen leveren, beheren en beveiligen van de Dienst;
- Het ondersteunen van gebruikers en het oplossen van incidenten;
- Het waarborgen van de beschikbaarheid en continuïteit van de dienst;
- Het uitvoeren van wettelijke en beveiligingsverplichtingen (logging, auditing).

Bijlage 2 Beschrijving van Persoonsgegevens & categorieën van Betrokkenen

1. In het kader van de opdracht worden de volgende Persoonsgegevens verwerkt:
- Identificatiegegevens — naam, e-mailadres;
- Authenticatiegegevens — inloggegevens, rollen, autorisaties;
- Contactgegevens — telefoonnummer, organisatie;
- Loggegevens — IP-adres, tijdstempels, systeemlogs;
- Gebruiksgegevens — acties in het systeem, foutmeldingen;
- Incidentgegevens — meldingen, tickets, communicatie;
- Configuratiegegevens — instellingen, voorkeuren.

2. In het kader van de opdracht betreft het de volgende categorieën van Betrokkenen:
- Gebruikers van Verantwoordelijke;
- Externe gebruikers (contractanten, leveranciers);
- Beheerders / functioneel beheerders.

3. De bewaartermijn van de Persoonsgegevens is als volgt:
- Loggegevens: 12 maanden na vastlegging;
- Incident- en ticketgegevens: 24 maanden na sluiting van het ticket;
- Gebruikersaccounts: 3 maanden na beëindiging van het account;
- Back-ups: volgens back-upcyclus, maximaal 6 maanden.

Verwerker verplicht zich hierbij om de Persoonsgegevens, zodra deze bewaartermijn(en) is/zijn verstreken, de betreffende Persoonsgegevens te vernietigen.

Bijlage 3 Maatregelen in verband met de meldplicht datalekken

1. In het geval van een Datalek zal Verwerker de Verantwoordelijke voorzien van alle door Verantwoordelijke verzochte relevante informatie met betrekking tot het Datalek. Deze informatie omvat in ieder geval:

    a. een beschrijving van de aard en de omvang van het Datalek, een inschatting van het aantal (mogelijk) getroffen Betrokkenen en een indicatie van de aard van de getroffen Persoonsgegevens en of deze Persoonsgegevens encrypted waren, dan wel anderszins beveiligd of onbegrijpelijk/ontoegankelijk waren gemaakt;

    b. een beschrijving van de getroffen en te treffen preventieve en correctieve maatregelen, geplande maatregelen en de aanbevolen maatregelen ter beperking van de schade, daaronder begrepen een noodplan en de verwachte oplossings- en work-around tijd;

    c. informatie over welke derden, zoals overheidsinstanties en de (sociale) media, bekend zijn of kunnen zijn met het Datalek;

    d. de contactgegevens van de bevoegde vertegenwoordiger(s) van Verwerker, bij wie Verantwoordelijke onmiddellijk en regelmatige updates kan verkrijgen van de status van het Datalek; en

    e. enige andere informatie die kan bijdragen aan de beperking van de schade aan de organisatie van Verantwoordelijke en de privacy van de getroffen Betrokkene(n).

2. Verwerker zal ook alle redelijkerwijs te verwachten assistentie aan Verantwoordelijke verlenen en alle noodzakelijke of door Verantwoordelijke gevraagde informatie met Verantwoordelijke delen, opdat Verantwoordelijke de (mogelijk) getroffen Betrokkene(n) en/of de toezichthouders die bevoegd zijn te oordelen over de Verwerking van de Persoonsgegevens, tijdig kan informeren over het Datalek en in staat wordt gesteld om naleving van de meldplichten inzake Datalekken onder de Geldende Privacywetgeving aan te aantonen.

Bijlage 4 Passende technische- en organisatorische maatregelen

Verantwoord omgaan met Persoonsgegevens valt of staat met een adequate beveiliging van de gegevens. De beveiliging hiervan dient te worden vastgelegd conform artikel 32 van de Algemene Verordening Gegevensbescherming. Hierin staat dat organisaties die Persoonsgegevens Verwerken, “passende technische en organisatorische maatregelen” nemen om Persoonsgegevens te beveiligen.

Uitwerking technische en organisatorische maatregelen

a. Passend beveiligingsniveau (technisch):

Verwerker voldoet aan de volgende technische normen:

ISO 2700x serie of vergelijkbaar niveau.

b. Passend beveiligingsniveau (organisatorisch):

- Opgeslagen informatie dient te worden beveiligd conform het veiligheidsniveau dat bij deze informatie is overeengekomen. Dit betekent onder meer dat:
  - ProRail vertrouwelijke informatie (zoals gegevens voor aanbestedingen en financiële gegevens) met Multi-factor authenticatie (of gelijkwaardig) beschermd moet zijn.
  - Persoonsgerelateerde informatie per definitie minimaal vertrouwelijk is (bij info over gezondheid: Geheim).
  - Laag vertrouwelijke informatie minimaal met wachtwoorden met voldoende sterkte dient te zijn afgeschermd.
  - Hoger vertrouwelijke informatie in een zogenaamde ongedeelde infrastructuur staat.

- Wat betreft Personeel betekent dit, dat:
  - Verwerker zich moet inspannen om er voor te zorgen dat medewerkers regelmatig op het belang van informatiebeveiliging wordt gewezen (security awareness).
  - Verwerker verantwoordelijk is voor alle betrokken medewerkers, inclusief ingehuurde personen, met autorisatierechten op de Infrastructuur van Verantwoordelijke. Een Verklaring Omtrent Gedrag (VOG) wordt sterk aanbevolen.
  - Iedere medewerker van Verwerker, met toegang tot de IT- systemen van Verantwoordelijke, bij aanvang schriftelijke informatie over het geldende informatiebeveiligingsbeleid krijgt.
  - Toegangsrechten tot informatie van Verantwoordelijke, van medewerkers van Verwerker die geen diensten verlenen aan Verantwoordelijke, per direct worden geblokkeerd.

c. Passend (fysieke) beveiligingsniveau serverruimte:

- In beheer zijnde apparatuur wordt in beveiligde ruimtes geplaatst. Deze beveiligde ruimtes zijn aantoonbaar alleen te benaderen door geautoriseerde personen.

Zie verder de eisen in 3.2.2 en 3.2.3 van het PvE.