DRIVEBACK

PRIVACY- EN INFORMATIEBEVEILIGING DOSSIER

DriveBack Europese Mobiliteitscontinuïteit
& DriveBack European Mortuary Services

AVG | AUTORISATIES | DATALEKKEN | GPS | DOSSIERBEHEER

Documentcode	DB-PIB-001
Versie	1.0
Uitgiftedatum	5 augustus 2026
Status	Volledige implementatiewerkversie
Classificatie	Intern en vertrouwelijk

Eén gedeelde beveiligingsbasis met afzonderlijke regels voor mobiliteitszaken en EMS-zaken.

DriveBack | Torenlaan 5, 1402 AT Bussum | 085 401 98 65

info@driveback.nl | ems@driveback.nl | www.driveback.nl

Documentbeheer en vaststelling

Dit dossier beschrijft het bindende interne kader zodra het formeel is goedgekeurd. Tot dat moment is het een volledige implementatiewerkversie en mogen open beslispunten niet stilzwijgend als vastgesteld beleid worden behandeld.

Onderdeel	Vastlegging
Juridische organisatie	DriveBack, eenmanszaak, KvK 42115463
Werkingsgebied	DriveBack Europese Mobiliteitscontinuïteit en DriveBack European Mortuary Services
Documenteigenaar	Directie / proceseigenaar privacy en informatiebeveiliging – J.B. Verdonk
Technisch eigenaar	IT- en systeemverantwoordelijke [IN TE VULLEN]
Privacycontact	Privacycoördinator of FG [IN TE VULLEN na FG-toets]
Reviewcyclus	Minimaal jaarlijks en direct na een zwaar incident, wetswijziging of systeemwijziging
Gerelateerde documenten	Operationele handboeken, Meldkamer- en Planningshandboek, Chauffeurs- en Personeelshandboek, contractenpakket, RI&E en continuïteitsplan

Goedkeuring

Directie / werkgever	J.B. Verdonk	**Datum**	01-10-2026
Privacyverantwoordelijke	J.B. Verdonk	**Datum**	01-10-2026
Informatiebeveiligingsverantwoordelijke	J.B. Verdonk	**Datum**	01-10-2026

Versiehistorie

Versie	Datum	Status	Wijziging	Eigenaar
0.1	5 augustus 2026	Concept	Eerste volledige structuur en beleidsinhoud	DriveBack
1.0	5 augustus 2026	Implementatiewerkversie	Compleet dossier voor juridische, organisatorische en technische implementatie	DriveBack
1.1	18 oktober 2026	Registratie vaststelling	Opgegeven ingangsdatum 01-10-2026 (met terugwerkende kracht); verificatie technische maatregelen loopt	J.B. Verdonk

Belangrijke juridische status

Dit document is geen bewijs van AVG-compliance, ISO/IEC 27001-certificering of toepasselijkheid van de Cyberbeveiligingswet. DriveBack moet aantoonbaar implementeren, testen, beheren en actualiseren. Waar “moet” staat, betreft dit een interne verplichting of een wettelijke verplichting die vooraf op toepasselijkheid moet zijn gecontroleerd.

Managementsamenvatting

DriveBack werkt 24/7 met locatiegegevens, reis- en voertuiggegevens, gegevens over ziekte of uitval, personeelsgegevens en - binnen EMS - gegevens van nabestaanden, opdrachtgevers, buitenlandse autoriteiten en ketenpartners. Beschikbaarheid is cruciaal voor de uitvoering; vertrouwelijkheid en juistheid zijn even belangrijk. Eén verkeerd gedeeld dossier, onbevoegde inzage, kwijtgeraakte telefoon of onnodig lang bewaarde GPS-route kan direct leiden tot veiligheidsrisico, reputatieschade, claims en meldplichten.

Kernbesluit

DriveBack hanteert één geïntegreerd privacy- en informatiebeveiligingsmanagementsysteem. Mobiliteitszaken, EMS-zaken en personeelszaken blijven logisch en technisch gescheiden. Toegang wordt per rol en per zaak toegekend, niet op basis van gemak of hiërarchie alleen.

Tien bestuurlijke uitgangspunten

1. De directie blijft eindverantwoordelijk voor privacy, cyberrisico's, continuïteit en leveranciersketen.
2. AFAS of de later formeel aangewezen centrale omgeving is de bronregistratie; losse mailboxen, privéapparaten en chatgesprekken zijn geen permanent dossier.
3. Iedere verwerking heeft een concreet doel, passende grondslag, minimale gegevensset, eigenaar en bewaartermijn.
4. Autorisaties volgen least privilege, functiescheiding, need-to-know en periodieke herbeoordeling.
5. MFA is verplicht voor externe toegang, beheerders, e-mail, cloud- en dossieromgevingen.
6. GPS wordt alleen gebruikt voor veiligheid, dispatch, aantoonbare uitvoering, incidentonderzoek en contractueel noodzakelijke rapportage; niet voor verborgen personeelscontrole.
7. Ieder mogelijk beveiligingsincident of datalek wordt direct intern gemeld; de 72-uursbeoordeling start zodra DriveBack kennis heeft van het incident.
8. EMS hanteert strengere toegang, minimale beeldregistratie, gesloten custody en waardige verwerking.
9. Back-ups zijn pas betrouwbaar na aantoonbare hersteltest; continuïteit omvat ook handmatige fallbackprocedures.
10. Managementreview, audits, oefeningen en corrigerende maatregelen vormen een vaste cyclus.

Prioriteiten vóór livegang

Prioriteit	Besluit of implementatie	Uitkomst / bewijs
P0	Benoem privacy- en beveiligingsverantwoordelijken en 24/7 incidentcontact	Mandaat, bereikbaarheidslijst, vervangingsregeling
P0	Stel systeemlandschap, bronregistratie, rollen en MFA definitief in	Goedgekeurde autorisatiematrix en technische test
P0	Sluit of actualiseer verwerkersovereenkomsten met AFAS, telefonie, cloud, GPS en overige leveranciers	Getekende overeenkomsten en subverwerkersregister
P0	Voer DPIA/LIA uit voor GPS, gespreksopnamen, monitoring en gevoelige EMS-/gezondheidsverwerkingen	Besluitenregister met restrisicoacceptatie
P0	Test datalekrespons, back-upherstel en crisiscommunicatie	Oefenverslag en CAPA
P1	Bepaal formeel of een FG verplicht of wenselijk is en of DriveBack onder de Cyberbeveiligingswet valt	Juridische toets en bestuursbesluit
P1	Bekrachtig bewaartermijnen en automatische verwijdering	Retentieconfiguratie en steekproef

Leeswijzer en gebruik

Het dossier is geschreven voor directie, meldkamer, planning, chauffeurs, EMS-crews, administratie, HR, IT-beheer, privacyfunctionaris, incidentteam en externe reviewers. Elk hoofdstuk bevat regels, een uitvoerbare werkinstructie, vereiste bewijsstukken en escalatiegronden.

Symbool / term	Betekenis
P0	Voorwaarde voor veilige en rechtmatige livegang; niet uitstellen.
P1	Binnen de eerste implementatiefase formeel vaststellen en aantoonbaar uitvoeren.
NO-GO	Werk, toegang, verzending of dispatch mag niet doorgaan.
HOLD	Tijdelijk blokkeren totdat een bevoegde functionaris een besluit vastlegt.
Legal hold	Gegevens niet wissen vanwege claim, onderzoek, geschil of wettelijk bevel.
Bronregistratie	Aangewezen systeem waarin de geldige, volledige en actuele zaakversie staat.
[IN TE VULLEN]	Besluit, naam, termijn of technische instelling die vóór formeel gebruik moet worden vastgesteld.

Voorrangsregel

Wet, toepasselijke cao, contractuele geheimhoudings- of beveiligingsafspraken en een schriftelijk besluit van een bevoegde autoriteit gaan vóór dit dossier. Afwijkingen worden vooraf beoordeeld, gemotiveerd en geregistreerd; mondelinge spoed is nooit een reden om bewijs achteraf weg te laten.

Inhoudsopgave

De paginanummers kunnen na latere wijzigingen in LibreOffice of Word worden bijgewerkt. De hoofdstukstructuur en documentcodes zijn leidend voor verwijzingen.

Onderdeel	Inhoud
Voorwerk	Documentbeheer, managementsamenvatting, leeswijzer en begrippen
Deel I	Besturing, rollen, toepasselijkheid en managementsysteem
Deel II	AVG: inventarisatie, grondslagen, DPIA, transparantie en rechten
Deel III	Dossierbeheer, bewaartermijnen, archivering en vernietiging
Deel IV	Autorisaties en technische/organisatorische informatiebeveiliging
Deel V	Beveiligingsincidenten, datalekken en crisisrespons
Deel VI	GPS, telematica, camera's, gespreksopnamen en monitoring
Deel VII	Bijzondere regels DriveBack Europese Mobiliteitscontinuïteit
Deel VIII	Bijzondere regels DriveBack European Mortuary Services
Deel IX	Personeelsprivacy en vertrouwelijkheid
Deel X	Audit, KPI's, training, testen en implementatie
Deel XI	Quick cards voor directe actie
Deel XII	Registers, beslismatrices en invulformulieren

Documentcodes

Reeks	Gebruik
DB-PIB-POL	Beleid en hoofdstukken in dit dossier
DB-PIB-QC	Quick cards
DB-PIB-F	Formulieren en registers
DB-PIB-IR	Incident- en datalekregistratie
DB-PIB-DPIA	DPIA- en LIA-dossiers
DB-PIB-ACC	Autorisatie- en toegangsbeheer
DB-PIB-RET	Bewaar-, vernietigings- en legal-holdregistratie
DB-PIB-SUP	Leveranciers- en verwerkersbeheer

Begrippen en afkortingen

Begrip	Definitie
AVG	Algemene verordening gegevensbescherming.
UAVG	Uitvoeringswet Algemene verordening gegevensbescherming.
AP	Autoriteit Persoonsgegevens.
Betrokkene	Geïdentificeerde of identificeerbare levende natuurlijke persoon op wie persoonsgegevens betrekking hebben.
Verwerkingsverantwoordelijke	Partij die doel en essentiële middelen van de verwerking bepaalt.
Verwerker	Partij die persoonsgegevens uitsluitend ten behoeve van en volgens instructie van de verantwoordelijke verwerkt.
FG	Functionaris voor gegevensbescherming; onafhankelijke toezichthoudende en adviserende functie wanneer verplicht of vrijwillig aangesteld.
Privacycoördinator	Interne uitvoerende rol zonder automatisch de onafhankelijke wettelijke positie van een FG.
DPIA	Data Protection Impact Assessment: voorafgaande beoordeling bij waarschijnlijk hoog privacyrisico.
LIA	Legitimate Interest Assessment: onderbouwde toets van gerechtvaardigd belang, noodzakelijkheid en belangenafweging.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare levende natuurlijke persoon.
Bijzondere persoonsgegevens	Onder meer gegevens over gezondheid, biometrie, ras/etniciteit, religie, politieke opvattingen en seksuele leven/gerichtheid.
Beveiligingsincident	Gebeurtenis die vertrouwelijkheid, integriteit of beschikbaarheid kan aantasten.
Datalek	Inbreuk in verband met persoonsgegevens: verlies, vernietiging, wijziging, ongeoorloofde verstrekking of toegang, al dan niet per ongeluk.
CIA	Confidentiality, Integrity, Availability: vertrouwelijkheid, integriteit en beschikbaarheid.
RBAC	Role-Based Access Control: toegang op basis van formele rol.
MFA	Multi-factor authentication.
JML	Joiner-Mover-Leaver: instroom, functiewijziging en uitdiensttreding.
MDM	Mobile Device Management.
SIEM	Security Information and Event Management.
RPO	Maximaal aanvaardbaar gegevensverlies in tijd.
RTO	Maximaal aanvaardbare hersteltijd.
EMS	DriveBack European Mortuary Services.
Custody	Aantoonbare keten van feitelijke verantwoordelijkheid en overdracht.
COMBI-zaak	Hoofdzaak met afzonderlijke mobiliteits- en EMS-subzaken.
Legal hold	Formele blokkade op verwijdering of wijziging vanwege onderzoek, claim, geschil of wettelijk bevel.
Cyberbeveiligingswet	Nederlandse implementatie van NIS2; toepasselijkheid moet op sector, omvang en rol worden getoetst.

DEEL I

BESTURING EN TOEPASSELIJKHEID

Governance, verantwoordelijkheden, managementsysteem en wettelijke reikwijdte

1. Doel, reikwijdte en beveiligingsprincipes

Dit dossier beschermt alle informatie die DriveBack ontvangt, maakt, gebruikt, deelt, bewaart of vernietigt bij mobiliteitscontinuïteit, EMS, personeel, financiën, leveranciers en bedrijfsvoering.

Kernregels

- Vertrouwelijkheid: alleen bevoegde personen krijgen toegang voor een aantoonbare taak.
- Integriteit: informatie is juist, volledig, herleidbaar en beschermd tegen onbevoegde wijziging.
- Beschikbaarheid: kritieke informatie en systemen zijn tijdig beschikbaar voor 24/7 hulpverlening.
- Rechtmatigheid en minimale verwerking: DriveBack verwerkt niet “voor de zekerheid” meer dan nodig.
- Veerkracht: beveiliging omvat preventie, detectie, respons, herstel en leren.

Werkinstructie

1. Bepaal vóór elke nieuwe verwerking het doel, de betrokkenen, de gegevenscategorieën en de eigenaar.
2. Classificeer informatie en bepaal de vereiste beschikbaarheid, vertrouwelijkheid en integriteit.
3. Leg grondslag, bewaartermijn, ontvangers, systemen en risico’s vast in het verwerkingsregister.
4. Implementeer passende organisatorische en technische maatregelen vóór livegang.
5. Evalueer de verwerking bij wijziging, incident, klacht, contractwijziging of ten minste jaarlijks.

Verplichte vastlegging

Verwerkingsregister, risicoregister, systeemeigenaar, proceseigenaar, besluit tot livegang en reviewdatum.

Direct escaleren of stoppen

Geen verwerking starten als doel, eigenaar, grondslag, toegang, beveiliging of bewaartermijn onbekend is.

2. Juridische entiteit en rolverdeling

De huidige contracterende en verwerkingsverantwoordelijke entiteit is DriveBack, eenmanszaak, tenzij per verwerking schriftelijk is vastgesteld dat DriveBack als verwerker of gezamenlijk verantwoordelijke handelt.

Kernregels

- De handelsnaam EMS creëert niet automatisch een afzonderlijke rechtspersoon of afzonderlijke AVG-rol.
- De feitelijke beslissingsmacht over doel en essentiële middelen bepaalt de privacyrol, niet alleen het contractlabel.
- Bij verwerking in opdracht van een verzekeraar, alarmcentrale of fleetklant wordt per proces een rolbeoordeling uitgevoerd.
- Bij gezamenlijke besluitvorming worden verantwoordelijkheden transparant verdeeld en vastgelegd.
- Een toekomstige B.V.-structuur vereist formele contract-, privacy- en datamigratiebesluiten.

Werkinstructie

1. Identificeer per proces wie het doel bepaalt, wie de middelen bepaalt en wie instructies geeft.
2. Classificeer de relatie als verantwoordelijke, verwerker, gezamenlijke verantwoordelijke of zelfstandige ontvanger.
3. Kies de juiste overeenkomst: dienstverlening, verwerkersovereenkomst, gegevensdelingsafspraak of gezamenlijke regeling.
4. Werk privacyverklaringen, verwerkingsregister en leveranciersregister bij.
5. Herbeoordeel de rol bij nieuwe opdrachtvoorwaarden, systemen, partners of holdingstructuur.

Verplichte vastlegging

Rolbeoordeling, ondertekende overeenkomst, privacyverklaring, registervermelding en goedkeuringsbesluit.

Direct escaleren of stoppen

Geen gegevensuitwisseling op basis van een generieke geheimhoudingsclausule als de privacyrollen en instructies niet duidelijk zijn.

3. Bestuurlijke verantwoordelijkheid en mandaten

De directie is eindverantwoordelijk voor privacy, informatiebeveiliging, continuïteit, leveranciersrisico en tijdige incidentbesluiten, ook wanneer uitvoering is uitbesteed.

Kernregels

- Beveiligingsrisico is een ondernemingsrisico en geen exclusief IT-onderwerp.
- Mandaten voor toegang, incidentmelding, AP-melding, communicatie en systeemwijzigingen zijn schriftelijk.
- Kritieke functies hebben een vervanger en 24/7-bereikbaarheidsregeling.
- Risicoacceptatie boven de vastgestelde grens mag alleen door de directie.
- Budget en capaciteit worden gekoppeld aan vastgestelde risico's en verbeterplannen.

Werkinstructie

1. Benoem proceseigenaar, informatie-eigenaar, systeemeigenaar, privacycontact en incidentleider.
2. Stel beslislimieten, vervanging en escalatievolgorde vast.
3. Bespreek privacy- en cyberrisico's ten minste per kwartaal in de managementreview.
4. Volg openstaande P0- en P1-maatregelen tot aantoonbare afsluiting.
5. Leg risicoacceptatie, afwijkingen en deadlines vast met naam en datum.

Verplichte vastlegging

Mandatenregister, RACI, managementreview, risicoacceptaties, budgetbesluiten en actielijst.

Direct escaleren of stoppen

Geen "stilzwijgende acceptatie": een onbeheerst hoog risico wordt gemitigeerd, vermeden, overgedragen of expliciet door de directie geaccepteerd.

4. Privacyorganisatie, FG-toets en onafhankelijk advies

DriveBack stelt een privacycoördinator aan en voert vóór livegang een formele toets uit of een Functionaris voor Gegevensbescherming wettelijk verplicht of organisatorisch wenselijk is.

Kernregels

- Een privacycoördinator mag uitvoering organiseren, maar is niet automatisch een onafhankelijke FG.
- Een eventuele FG krijgt tijdig toegang tot bestuur, informatie, middelen en alle verwerkingen.
- De FG mag geen functie vervullen die doelen en middelen van verwerking bepaalt.
- Adviezen, afwijkingen en bestuurlijke besluiten worden schriftelijk bewaard.
- Contactgegevens voor privacyvragen zijn intern en extern duidelijk.

Werkinstructie

1. Voer de FG-noodzaakstoets uit op kerntaken, aard, schaal, stelselmatige observatie en bijzondere gegevens.
2. Leg conclusie, feiten, juridische beoordeling en herbeoordelingsdatum vast.
3. Benoem bij geen FG minimaal een privacycoördinator met mandaat en directe escalatielijn.
4. Richt een onafhankelijk advies- en rapportageproces in.
5. Herhaal de toets bij schaalgroei, nieuw dataplatform, uitbreiding EMS, grootschalige GPS-monitoring of nieuwe wettelijke verplichting.

Verplichte vastlegging

FG-toets, benoemingsbesluit, functieomschrijving, contactpublicatie, adviesregister en jaarlijkse evaluatie.

Direct escaleren of stoppen

Noem een medewerker niet “FG” zonder formele positie, onafhankelijkheid en eventuele aanmelding bij de AP.

5. Informatiebeveiligingsmanagementsysteem

DriveBack beheert beveiliging als een herhaalbare cyclus van context, risicoanalyse, maatregelen, uitvoering, monitoring, audit en verbetering, aansluitend op ISO/IEC 27001-principes zonder certificeringsclaim.

Kernregels

- De scope omvat mensen, processen, systemen, voertuigen, papier, locaties, leveranciers en informatie in iedere vorm.
- Risicobehandeling is gekoppeld aan eigenaarschap, deadline, bewijs en restrisico.
- Maatregelen zijn proportioneel aan impact en waarschijnlijkheid.
- Effectiviteit wordt gemeten; alleen aanwezigheid van beleid is onvoldoende.
- Wijzigingen worden vooraf beoordeeld op security en privacy by design.

Werkinstructie

1. Bepaal context, belanghebbenden, kritieke processen en systeemscope.
2. Onderhoud een informatieassetregister en risicoanalyse.
3. Kies maatregelen, leg uitzonderingen vast en wijs eigenaren toe.
4. Voer controles, monitoring, incidentrespons, oefeningen en audits uit.
5. Bespreek resultaten in managementreview en verbeter via corrigerende maatregelen.

Verplichte vastlegging

ISMS-scope, assetregister, risicoregister, maatregelenplan, auditverslagen, KPI’s, managementreview en CAPA-register.

Direct escaleren of stoppen

Gebruik termen als “ISO/IEC 27001-geïnspireerd” of “aansluitend op principes”; communiceer geen certificering zonder geldig certificaat.

6. Classificatie van informatie

Alle informatie krijgt een beschermingsniveau dat bepaalt wie toegang krijgt, hoe overdracht plaatsvindt, waar opslag is toegestaan en hoe vernietiging gebeurt.

Kernregels

- OPENBAAR: goedgekeurd voor externe publicatie.
- INTERN: voor medewerkers en geautoriseerde opdrachtnemers.
- VERTROUWELIJK: klant-, personeels-, contract-, financiële en operationele informatie op need-to-knowbasis.

- ZEER VERTROUWELIJK: gezondheidsgegevens, identiteitskopieën, EMS-custody, incidentonderzoek, beheeraccounts en juridische dossiers.
- Classificatie volgt de hoogste gevoeligheid in het document of dossier.

Werkinstructie

1. Classificeer bij creatie of ontvangst en leg eigenaar vast.
2. Gebruik herkenbare labels in dossier, onderwerpregel, bestandsnaam of metadata.
3. Pas kanaal, encryptie, deelrechten en bewaartermijn aan de classificatie aan.
4. Herclassificeer na anonimisering, publicatiebesluit of einde gevoeligheid.
5. Vernietig volgens de strengste toepasselijke methode en registreer waar vereist.

Verplichte vastlegging

Classificatielabel, eigenaar, toegangsprofiel, deelhistorie en vernietigingsbewijs.

Direct escaleren of stoppen

ZEER VERTROUWELIJKE informatie mag niet via privé-e-mail, onbeheerde chat, publieke deel-link of onbeheerd apparaat worden verwerkt.

7. Rollen, functiescheiding en RACI

Taken worden zo verdeeld dat één persoon niet onbeperkt een zaak kan aanmaken, autoriseren, betalen, wijzigen, exporteren en wissen zonder controle.

Kernregels

- Directie stelt beleid, risicoacceptatie en meldbesluiten vast.
- Meldkamer en planning verwerken alleen zaakgegevens die nodig zijn voor intake, dispatch en bewaking.
- Chauffeurs en EMS-crews zien uitsluitend de operationele opdrachtset voor hun inzet.
- Administratie ziet financiële bewijsstukken en minimale operationele referenties.
- IT-beheer beheert techniek, maar leest inhoud alleen bij aantoonbare noodzaak en logging.

Werkinstructie

1. Maak per proces een RACI met Responsible, Accountable, Consulted en Informed.
2. Identificeer conflicterende bevoegdheden en voeg vierogencontrole toe.
3. Koppel rollen aan systemen en dossiercategorieën.
4. Test met representatieve accounts of toegang werkelijk overeenkomt met de matrix.
5. Herbeoordeel bij functiewijziging, uitbreiding, incident en minimaal halfjaarlijks.

Verplichte vastlegging

RACI, functiescheidingsmatrix, testaccounts, reviewverslag en uitzonderingsregister.

Direct escaleren of stoppen

Een leidinggevende krijgt niet automatisch onbeperkte dossierinzage; hiërarchie is geen vervanging voor need-to-know.

8. Wettelijk en contractueel normenkader

DriveBack onderhoudt één actueel register van AVG/UAVG, arbeidsrechtelijke privacyregels, telecommunicatie- en cameraregels, contractuele beveiligingseisen, verzekeringsvoorwaarden, Cyberbeveiligingswettoets en relevante normen.

Kernregels

- Wetswijzigingen worden vertaald naar concrete processen, niet alleen opgeslagen als bron.

- Contractuele eisen kunnen strenger zijn dan de interne basis en worden per klant gemarkeerd.
- Buitenlandse opdrachten vereisen toetsing van lokale document- en doorgifteregels.
- Bronnen worden beoordeeld op autoriteit, datum en toepasselijkheid.
- Juridisch advies en technische interpretatie worden bewaard bij het besluit.

Werkinstructie

1. Benoem eigenaar voor juridische en normatieve actualiteiten.
2. Controleer officiële bronnen minimaal per kwartaal en bij nieuwe diensten.
3. Registreer wijziging, impact, verantwoordelijke en implementatiedatum.
4. Werk beleid, contracten, privacyinformatie, systemen en training bij.
5. Verifieer effectiviteit en sluit de wijziging formeel af.

Verplichte vastlegging

Wet- en normregister, impactanalyse, wijzigingsbesluit, bijgewerkte documenten en opleidingsbewijs.

Direct escaleren of stoppen

Een internetartikel of leverancierstekst is geen voldoende juridische basis wanneer officiële wet, toezichthouder of contract beschikbaar is.

9. Cyberbeveiligingswet: toepasselijkheid en overgang

DriveBack beoordeelt vóór 15 augustus 2026 formeel of de onderneming door sector, omvang, rol, verbonden ondernemingen of bijzondere aanwijzing onder de Cyberbeveiligingswet valt.

Kernregels

- Toepasselijkheid wordt niet aangenomen of uitgesloten op basis van bedrijfsnaam alleen.
- De toets omvat sector vervoer, eventuele digitale diensten, omvangscriteria, groepsstructuur en uitzonderingen.
- Ook buiten formele toepasselijkheid worden redelijke NIS2-principes gebruikt voor weerbaarheid en leveranciersketen.
- Bij toepasselijkheid zijn registratie, zorgplicht, incidentmelding en bestuurlijke verantwoordelijkheid onderdeel van het implementatieplan.
- De uitkomst wordt jaarlijks en bij schaal- of structuurwijziging herzien.

Werkinstructie

1. Gebruik de officiële doorverwijsboom en leg feiten over sector, activiteiten, werknemers, omzet en balanstotaal vast.
2. Laat de conclusie juridisch toetsen wanneer twijfel bestaat.
3. Registreer tijdig wanneer DriveBack onder de wet valt.
4. Richt meldtermijnen, bestuurstraining, risicobeheer en leveranciersbeheersing in.
5. Test de Cbw-respons naast de AVG-datalekrespons.

Verplichte vastlegging

Cbw-toets, bestuursbesluit, registratiebewijs indien van toepassing, zorgplichtplan, meldmatrix en trainingsbewijs.

Juridisch aandachtspunt

De Cbw-toets in dit dossier is een implementatiepoort; zij vervangt geen juridisch advies.

Direct escaleren of stoppen

Omdat de wet op 15 augustus 2026 in werking treedt, mag een onvoltooide toepasselijkheidstoets na die datum niet als “nog niet relevant” blijven staan.

10. Beleidscyclus, uitzonderingen en wijzigingsbeheer

Privacy- en beveiligingsbeleid blijft alleen betrouwbaar wanneer wijzigingen gecontroleerd worden doorgevoerd en tijdelijke uitzonderingen een eigenaar, einddatum en compensatie hebben.

Kernregels

- Iedere beleidsversie heeft eigenaar, datum, status, goedkeuring en verspreidingslijst.
- Uitzonderingen zijn specifiek, tijdelijk, risicogebaseerd en herroepbaar.
- Systeemwijzigingen doorlopen security- en privacybeoordeling vóór productie.
- Noodwijzigingen worden achteraf binnen één werkdag gereviewd.
- Verouderde versies worden ingetrokken maar volgens documentbeheer bewaard.

Werkinstructie

1. Dien wijzigingsverzoek in met aanleiding, scope, risico en testplan.
2. Beoordeel privacy, security, continuïteit, contract en opleiding.
3. Laat bevoegde eigenaar goedkeuren en plan implementatie/rollback.
4. Test technisch én met gebruikers; registreer bevindingen.
5. Publiceer, instrueer, archiveer vorige versie en plan evaluatie.

Verplichte vastlegging

Wijzigingsverzoek, impactanalyse, goedkeuring, testverslag, uitrolbewijs, communicatie en reviewdatum.

Direct escaleren of stoppen

Een langdurige “tijdelijke” uitzondering zonder eigenaar en einddatum wordt behandeld als onbeheerst risico en geëscaleerd.

DEEL II

AVG EN GEGEVENSVERWERKING

Verwerkingsregister, grondslagen, gevoelige gegevens, DPIA, transparantie en rechten

11. Gegevensinventarisatie en dataflowmapping

DriveBack kent per proces welke gegevens binnenkomen, waar zij vandaan komen, door welke systemen en partijen zij lopen, wie toegang heeft, waar zij worden opgeslagen en wanneer zij worden verwijderd.

Kernregels

- De inventaris omvat digitale, papieren, mondelinge, telefonische, voertuig- en GPS-gegevens.
- Shadow IT, exports, downloads, lokale mappen en tijdelijke chatbestanden worden expliciet meegenomen.
- Dataflows tonen ook overdracht naar buitenlandse partners en subverwerkers.
- Koppelingen en automatische synchronisaties hebben een eigenaar en doel.
- Onbekende of niet-goedgekeurde gegevensstromen worden geblokkeerd.

Werkinstructie

1. Inventariseer processen, formulieren, mailboxen, apps, telefoons, voertuigen, cloudsystemen en papieren archieven.
2. Noteer bron, bestemming, systeem, ontvanger, frequentie, beveiliging en bewaartermijn.
3. Markeer bijzondere gegevens, locatiegegevens, identiteitsdocumenten en gegevens van minderjarigen.
4. Valideer de kaart met meldkamer, planning, EMS, HR, administratie en IT.
5. Werk de kaart bij vóór iedere nieuwe koppeling, leverancier of dienstverlening.

Verplichte vastlegging

Dataflowdiagram, systeemregister, gegevenscategorieën, ontvangerslijst, koppelingenregister en reviewbewijs.

Direct escaleren of stoppen

Geen koppeling, export of synchronisatie activeren wanneer eigenaar, doel, beveiliging of verwijderroute ontbreekt.

12. Register van verwerkingsactiviteiten

Het verwerkingsregister is het centrale bewijs van welke persoonsgegevens DriveBack verwerkt en vormt de basis voor privacyverklaringen, DPIA's, contracten, beveiligingsmaatregelen en bewaartermijnen.

Kernregels

- Iedere terugkerende verwerking krijgt een unieke registercode.
- Het register onderscheidt verantwoordelijke- en verwerkersactiviteiten.
- Doelen, categorieën, ontvangers, doorgiften, termijnen en beveiliging zijn concreet.
- Werkelijke systemen en partners worden genoemd; generieke termen als "IT" zijn onvoldoende.

- Wijzigingen worden gedateerd en door een eigenaar goedgekeurd.

Werkinstructie

1. Maak een registerregel vóór livegang van een proces.
2. Koppel iedere regel aan proces, grondslag, privacyinformatie, risico en bewaartermijn.
3. Controleer halfjaarlijks met proceseigenaren of de praktijk overeenkomt.
4. Corrigeer afwijkingen en verwijder beëindigde verwerkingen volgens legal-holdregels.
5. Gebruik het register bij verzoeken, incidenten, audits en leveranciersbeoordeling.

Verplichte vastlegging

Actueel verwerkingsregister, wijzigingslog, proceseigenaar, reviewdatum en koppeling naar relevante documenten.

Direct escaleren of stoppen

Een niet-geregistreerde structurele verwerking krijgt HOLD totdat registratie en beoordeling zijn afgerond.

13. Categorieën betrokkenen en gegevens

DriveBack classificeert betrokkenen en gegevens zodat grondslag, informatieplicht, toegang, beveiliging en bewaartermijn passend kunnen worden bepaald.

Kernregels

- Betrokkenen kunnen zijn: melders, bestuurders, passagiers, minderjarigen, voertuigeigenaren, nabestaanden, contactpersonen, medewerkers en partners.
- Gegevenscategorieën omvatten identificatie, contact, locatie, reis, voertuig, financieel, contractueel, communicatie, incident en gezondheid.
- Identiteitsnummers, kopieën, gezondheidsgegevens en strafrechtelijke gegevens krijgen verhoogde bescherming.
- Gegevens over overledenen vallen niet rechtstreeks onder de AVG, maar gegevens over levende nabestaanden en betrokkenen wel.
- Combinaties van gewone gegevens kunnen alsnog zeer gevoelig zijn.

Werkinstructie

1. Koppel iedere gegevenscategorie aan een concrete noodzaak in het proces.
2. Markeer bijzondere en hoog-risicocategorieën in formulieren en systemen.
3. Beperk vrije tekstvelden en gebruik gestructureerde keuzes waar mogelijk.
4. Voorkom dat medische diagnoses, familierelaties of emotionele details zonder noodzaak worden vastgelegd.
5. Herzie de dataset na incidenten, klachten en proceswijzigingen.

Verplichte vastlegging

Datacatalogus, velddefinities, classificatie, noodzaakstoets en verwijderbesluit voor overbodige velden.

Direct escaleren of stoppen

Geen kopie identiteitsdocument, medische diagnose of foto van een overledene verzamelen als een minder ingrijpende verificatie volstaat.

14. Doelbinding en minimale gegevensverwerking

Persoonsgegevens worden uitsluitend gebruikt voor vooraf bepaalde, uitdrukkelijke en gerechtvaardigde doelen en niet hergebruikt voor onverenigbare doeleinden.

Kernregels

- Een operationeel dossier is geen marketingbestand.
- Een GPS-route voor veiligheid wordt niet zonder nieuwe beoordeling gebruikt voor prestatiebeoordeling.

- EMS-informatie wordt niet gebruikt voor publiciteit, training of beeldmateriaal zonder afzonderlijke wettelijke basis en waardigheidstoets.
- Vrije aantekeningen blijven feitelijk, noodzakelijk en professioneel.
- Testdata bevat geen echte persoonsgegevens tenzij aantoonbaar noodzakelijk en beschermd.

Werkinstructie

1. Beschrijf het primaire doel in één duidelijke zin.
2. Bepaal per gegevensveld of het nodig en proportioneel is.
3. Beoordeel hergebruik op verenigbaarheid, verwachting, context en risico.
4. Informeer betrokkenen en pas grondslag/maatregelen aan wanneer nieuw gebruik rechtmatig is.
5. Verwijder velden, exports en duplicaten die geen actief doel meer hebben.

Verplichte vastlegging

Doelomschrijving, veldinventaris, hergebruikbeoordeling, bijgewerkte privacyinformatie en verwijderbewijs.

Direct escaleren of stoppen

Gebruik gegevens niet “omdat ze beschikbaar zijn”; zonder aantoonbare noodzaak volgt blokkering of verwijdering.

15. Grondslagen en contractuele noodzaak

Iedere verwerking van persoonsgegevens steunt op een geldige AVG-grondslag die past bij het werkelijke doel; toestemming wordt niet als gemakkelijke standaard gebruikt.

Kernregels

- Overeenkomst: noodzakelijk voor uitvoering of precontractuele stappen op verzoek van de betrokkene.
- Wettelijke verplichting: concrete wettelijke bepaling wordt geregistreerd.
- Gerechtvaardigd belang: vereist LIA met noodzaak, proportionaliteit en belangenafweging.
- Vitaal belang: alleen in echte noodsituaties en wanneer geen minder ingrijpende basis volstaat.
- Toestemming: vrij, specifiek, geïnformeerd, ondubbelzinnig en aantoonbaar; intrekking is even eenvoudig.

Werkinstructie

1. Bepaal doel en relatie met de betrokkene.
2. Kies de meest passende grondslag en motiveer waarom alternatieven niet passen.
3. Controleer aanvullende voorwaarden voor bijzondere gegevens.
4. Leg de grondslag vast in register, formulier en privacyinformatie.
5. Herbeoordeel wanneer doel, relatie of dataset verandert.

Verplichte vastlegging

Grondslagenmatrix, verwijzing naar wet of contract, LIA/toestemmingsbewijs en reviewdatum.

Direct escaleren of stoppen

Noem “toestemming” niet als grondslag wanneer dienstverlening feitelijk afhankelijk is en weigering geen echte vrije keuze biedt.

16. Bijzondere persoonsgegevens, gezondheid en strafrechtelijke gegevens

Gezondheids- en andere bijzondere gegevens worden alleen verwerkt wanneer naast een gewone grondslag ook een toepasselijke uitzondering op het verwerkingsverbod bestaat.

Kernregels

- DriveBack registreert bij uitval alleen operationeel noodzakelijke beperkingen en bewijsstatus, niet automatisch diagnose of medisch dossier.
- Werkgever en leidinggevende ontvangen geen medische details die bij bedrijfsarts of arbodienst horen.
- In EMS worden infectie- en blootstellingsrisico's beperkt tot wat nodig is voor veilige uitvoering.
- Strafrechtelijke gegevens en VOG-status worden alleen onder toepasselijke voorwaarden verwerkt.
- Toegang, logging, export en retentie zijn strenger dan voor gewone zaakgegevens.

Werkinstructie

1. Bepaal of de informatie werkelijk bijzonder of strafrechtelijk is.
2. Leg grondslag én uitzondering vast voordat verwerking structureel start.
3. Vraag alleen de functionele informatie die de taak vereist.
4. Beperk toegang tot benoemde rollen en controleer inzage.
5. Verwijder of anonimiseer zodra het doel is bereikt, tenzij een concrete bewaarplicht geldt.

Verplichte vastlegging

Bijzondere-gegevensregister, rechtsgrond, autorisatielijst, inzagelog en verwijderbewijs.

Juridisch aandachtspunt

Voor bijzondere persoonsgegevens volstaat een gewone AVG-grondslag niet; de aanvullende wettelijke uitzondering moet eveneens vaststaan.

Direct escaleren of stoppen

Een diagnose, medicatielijst, doodsoorzaak of infectiestatus mag niet uit nieuwsgierigheid of "voor volledigheid" in vrije tekst worden opgenomen.

17. Gegevens over overledenen en levende betrokkenen

De AVG beschermt gegevens van overleden personen niet rechtstreeks, maar dezelfde dossiers bevatten vaak persoonsgegevens van nabestaanden, melders, artsen, chauffeurs en andere levende personen. DriveBack hanteert daarom één waardig en streng beschermingsregime.

Kernregels

- Geen lagere beveiliging alleen omdat de hoofdzaak een overledene betreft.
- Nabestaanden krijgen duidelijke informatie over hun eigen gegevens en communicatie.
- Doodsoorzaak, omstandigheden en familiegegevens worden alleen verwerkt voor noodzakelijke uitvoering.
- Contractuele geheimhouding, beroepsnormen, waardigheid en andere wettelijke regels blijven gelden.
- Openbaarmaking, training en beeldgebruik zijn uitgesloten zonder afzonderlijke beoordeling.

Werkinstructie

1. Scheid gegevens over de overledene van persoonsgegevens van levende betrokkenen waar praktisch mogelijk.
2. Classificeer EMS-dossiers standaard ZEER VERTROUWELIJK.
3. Bepaal per ontvanger welke minimale informatie nodig is.
4. Registreer iedere custody- en gegevensoverdracht.
5. Beoordeel inzage- of correctieverzoeken op wiens gegevens het verzoek ziet.

Verplichte vastlegging

EMS-dossierclassificatie, ontvangerslog, custodyregistratie, privacyverzoekbeoordeling en geheimhoudingsafspraken.

Direct escaleren of stoppen

De mededeling "de AVG geldt niet voor overledenen" mag nooit worden gebruikt om dossierbeveiliging, waardigheid of rechten van levende betrokkenen te negeren.

18. Gerechtvaardigd belang en LIA

Wanneer DriveBack zich op gerechtvaardigd belang beroept, wordt vooraf aantoonbaar getoetst of het belang legitiem, de verwerking noodzakelijk en de impact op betrokkenen evenwichtig is.

Kernregels

- Het belang wordt concreet beschreven; “bedrijfsbelang” is te vaag.
- Noodzakelijkheid omvat toetsing van minder ingrijpende alternatieven.
- Verwachtingen, machtsverhouding, kwetsbaarheid, omvang en bezwaarrecht worden meegewogen.
- Mitigerende maatregelen zijn onderdeel van de uitkomst.
- Een LIA wordt herhaald bij andere doelen, intensievere monitoring of nieuwe technologie.

Werkinstructie

1. Beschrijf belang, begunstigde en maatschappelijk/zakelijk gewicht.
2. Toets causaal verband en noodzakelijkheid.
3. Inventariseer impact, redelijke verwachtingen en risico’s voor betrokkenen.
4. Bepaal maatregelen zoals kortere retentie, uitschakelbaarheid, beperkte toegang en transparantie.
5. Laat een bevoegde functionaris beslissen en leg bezwaarroute vast.

Verplichte vastlegging

LIA-formulier, alternatievenanalyse, restrisico, besluit, privacyinformatie en reviewdatum.

Direct escaleren of stoppen

GPS- of personeelsmonitoring mag niet live wanneer de LIA slechts uit een algemene zin bestaat of werknemers niet vooraf zijn geïnformeerd.

19. Toestemming en bewijsbeheer

Toestemming wordt alleen gebruikt wanneer de betrokkene echt vrij kan kiezen en weigering of intrekking geen ongeoorloofde nadelige gevolgen heeft.

Kernregels

- Toestemming is gescheiden van algemene voorwaarden en per doel specifiek.
- Stilte, vooraf aangevinkte vakjes of algemene akkoordverklaringen zijn onvoldoende.
- Intrekking stopt toekomstig gebruik zonder onnodige drempels.
- Bewijs bevat versie, datum, doel, informatie en wijze van toestemming.
- Voor minderjarigen wordt leeftijd en eventuele ouderlijke bevoegdheid beoordeeld.

Werkinstructie

1. Bepaal of toestemming werkelijk passend is en documenteer alternatieven.
2. Geef begrijpelijke informatie vóór de keuze.
3. Registreer actieve handeling, datum, versie en kanaal.
4. Richt intrekking en technische blokkering in.
5. Verwijder of hergrond gegevens na intrekking; documenteer de uitkomst.

Verplichte vastlegging

Toestemmingsregister, informatietekstversie, intrekking, blokkering en verwijder-/hergrondbesluit.

Direct escaleren of stoppen

Gebruik toestemming niet als noodverband voor verwerking die feitelijk contractueel verplicht of structureel personeelsgericht is.

20. Privacy by design en privacy by default

Nieuwe diensten, formulieren, voertuigsystemen, apps, koppelingen en workflows worden zo ontworpen dat minimale gegevens, korte standaardretentie en beperkte toegang de standaard zijn.

Kernregels

- Optionele velden staan standaard uit of leeg.
- Publieke deel-links, brede groepsrechten en permanente tracking staan standaard uit.
- Test- en acceptatieomgevingen gebruiken geanonimiseerde of synthetische data.
- Exportfuncties, logging, verwijdering en rechtenafhandeling worden vóór livegang getest.
- Leveranciersselectie weegt privacy en security vanaf de offertestap.

Werkinstructie

1. Start ieder project met gegevens- en risico-inventarisatie.
2. Leg privacy- en beveiligingseisen vast in ontwerp en inkoop.
3. Voer LIA/DPIA en leveranciersbeoordeling uit waar nodig.
4. Test standaardinstellingen, rollen, logging, retentie en herstel.
5. Laat privacy en security formeel goedkeuren vóór productie.

Verplichte vastlegging

Ontwerpchecklist, requirements, DPIA/LIA, testverslag, acceptatiebesluit en technische configuratie.

Direct escaleren of stoppen

Geen livegang met standaardbeheerwachtwoord, onbeperkte retentie, brede toegang of ontbrekende verwijderfunctie.

21. DPIA en voorafgaande raadpleging

Een DPIA wordt uitgevoerd vóór verwerkingen die waarschijnlijk een hoog privacyrisico opleveren, waaronder intensieve locatievolging, nieuwe monitoring, grootschalige gevoelige gegevens of combinatie van kwetsbare groepen en technologie.

Kernregels

- De DPIA start vóór aanschaf of configuratie, niet na volledige implementatie.
- Betrokken proceseigenaren, IT, privacy en waar passend medewerkersvertegenwoordiging worden gehoord.
- Risico’s voor rechten en vrijheden staan centraal, niet alleen bedrijfsrisico.
- Maatregelen worden getest en restrisico wordt expliciet beoordeeld.
- Bij blijvend hoog restrisico volgt voorafgaande raadpleging van de AP.

Werkinstructie

1. Voer een DPIA-screening uit voor ieder nieuw of gewijzigd hoog-risicoproces.
2. Beschrijf verwerking, noodzaak, proportionaliteit, betrokkenen, gegevensstromen en risico’s.
3. Bepaal maatregelen, eigenaar, deadline en testmethode.
4. Laat onafhankelijke privacybeoordeling en bestuursbesluit vastleggen.
5. Herhaal bij materiële wijziging of maximaal iedere drie jaar voor risicovolle verwerkingen.

Verplichte vastlegging

DPIA-screening, volledige DPIA, maatregelenplan, testbewijs, restrisicoacceptatie en eventuele AP-correspondentie.

Juridisch aandachtspunt

Een DPIA is wettelijk verplicht wanneer de verwerking waarschijnlijk een hoog privacyrisico oplevert.

Direct escaleren of stoppen

GPS, gespreksopnamen, cameratoezicht of EMS-verwerking met hoog risico mogen niet worden ingevoerd zolang verplichte DPIA en maatregelen ontbreken.

22. Transparantie en privacyverklaringen

Betrokkenen ontvangen tijdig, begrijpelijk en doelgroepgericht informatie over wie DriveBack is, welke gegevens worden verwerkt, waarom, met wie, hoe lang, welke rechten gelden en hoe zij contact opnemen.

Kernregels

- Er zijn afzonderlijke of modulair opgebouwde verklaringen voor klanten, website, sollicitanten, medewerkers, GPS/voertuigen en EMS.
- Informatie wordt gegeven op het moment van verkrijging of binnen de toepasselijke termijn bij indirecte verkrijging.
- Spoed verhindert niet dat informatie zo snel mogelijk wordt verstrekt.
- Juridische tekst wordt vertaald naar duidelijke praktische taal.
- Versies en publicatiedata worden bewaard.

Werkinstructie

1. Koppel iedere registerregel aan een privacyverklaring of specifieke informatiekaart.
2. Controleer of doelen, ontvangers, doorgiften en termijnen overeenkomen met de praktijk.
3. Publiceer via passend kanaal en geef operationele informatie tijdens intake of onboarding.
4. Registreer wanneer uitzonderingen op informatieplicht worden toegepast.
5. Werk verklaringen bij vóór materiële verandering en communiceer relevante wijzigingen.

Verplichte vastlegging

Privacyverklaringen, versielog, publicatiebewijs, scripts, intakebevestiging en uitzonderingsbesluit.

Direct escaleren of stoppen

Een algemene websiteverklaring vervangt niet de specifieke informatie die nodig is bij personeelsmonitoring, GPS of EMS-gegevensuitwisseling.

23. Rechten van betrokkenen en verificatie

DriveBack behandelt verzoeken om inzage, correctie, verwijdering, beperking, overdraagbaarheid, bezwaar en informatie binnen de wettelijke termijn en zonder onnodige drempels.

Kernregels

- De identiteit wordt proportioneel geverifieerd; standaard een volledige ID-kopie vragen is niet toegestaan.
- De reactietermijn is in beginsel één maand; verlenging wordt tijdig gemotiveerd.
- Rechten van anderen, geheimhouding, juridische claims en wettelijke uitzonderingen worden zorgvuldig afgewogen.
- Systemen en leveranciers worden meegenomen zodat een antwoord volledig is.
- Afwijzing is gemotiveerd en bevat klacht- en beroepsmogelijkheden.

Werkinstructie

1. Registreer verzoek, datum, reikwijdte en gewenste communicatie.
2. Verifieer identiteit via bestaand kanaal, dossierkennis of beperkte aanvullende controle.
3. Zoek in alle relevante systemen, mailboxen, dossiers, logs en verwerkers.
4. Laat juridische/privacyreview uitvoeren en pas noodzakelijke redactie toe.
5. Reageer, voer acties uit en archiveer bewijs van afronding.

Verplichte vastlegging

Verzoekenregister, identiteitsverificatie, zoeklog, besluit, verstrekte kopie, verwijder-/correctiebewijs en termijnbewaking.

Direct escaleren of stoppen

Escaleren wanneer identiteit onzeker is, meerdere personen in één EMS-dossier voorkomen, een claim/legal hold geldt of de termijn dreigt te verlopen.

24. Privacyklachten, toezicht en correspondentie

Privacyklachten worden onafhankelijk, respectvol en aantoonbaar onderzocht; correspondentie met de AP of andere toezichthouder wordt centraal beheerd.

Kernregels

- Een klacht is geen reden om dossiergegevens te verwijderen voordat onderzoek en legal-holdbeoordeling zijn afgerond.
- Klager ontvangt ontvangstbevestiging, contactpersoon en verwachte vervolgstap.
- Onderzoek scheidt feiten, beoordeling, herstel en communicatie.
- Structurele oorzaken leiden tot CAPA en managementreview.
- Toezichthouderverzoeken krijgen direct juridische en bestuurlijke prioriteit.

Werkinstructie

1. Registreer klacht of toezichthoudercontact dezelfde werkdag.
2. Benoem onafhankelijke behandelaar en beveilig relevante bewijsstukken.
3. Onderzoek proces, logs, communicatie, grondslag, toegang en leveranciers.
4. Besluit over herstel, melding, excuses, compensatie of beleidswijziging.
5. Communiceer gemotiveerd en sluit pas na verificatie van maatregelen.

Verplichte vastlegging

Klachtenregister, onderzoek, bewijs, communicatie, besluit, CAPA en managementrapportage.

Direct escaleren of stoppen

Direct escaleren bij dreigende toezichthoudertermijn, vermoedelijke stelselmatige overtreding, misleiding of hoog risico voor kwetsbare betrokkenen.

DEEL III

DOSSIERBEHEER EN BEWAARTERMIJNEN

Zaakstructuur, bronregistratie, documenten, beeld, delen, archiveren en vernietigen

25. Zaakarchitectuur: Mobiliteit, EMS en COMBI

Iedere opdracht krijgt een unieke zaakstructuur waarin gegevens logisch gescheiden, herleidbaar en alleen voor bevoegde rollen zichtbaar zijn.

Kernregels

- Mobiliteitszaken gebruiken een DBM-zaakcode; EMS-zaken een EMS-zaakcode.
- Een gecombineerde opdracht krijgt één COMBI-hoofdzaak met afzonderlijke DBM- en EMS-subzaken.
- Financiële en contactgegevens mogen via gecontroleerde referenties worden gekoppeld, niet door volledige dossiers te dupliceren.
- EMS-toegang wordt niet automatisch verleend aan mobiliteitsmedewerkers en omgekeerd.
- Zaakstatus, eigenaar, prioriteit en retentiecategorie zijn verplichte metadata.

Werkinstructie

1. Maak de zaak aan in de bronregistratie en genereer de juiste unieke code.
2. Selecteer dienststroom, opdrachtgever, betrokkenen, risicoklasse en gegevensclassificatie.
3. Koppel subzaken alleen wanneer operationeel noodzakelijk en autoriseer rollen afzonderlijk.
4. Controleer vóór dispatch of de juiste opdrachtset is gepubliceerd.
5. Sluit hoofd- en subzaken pas na volledige overdracht, kostencontrole en dossiercontrole.

Verplichte vastlegging

Zaaknummer, subzaakrelatie, rollen, statuslog, dispatchset, overdracht en afsluitcheck.

Direct escaleren of stoppen

Geen EMS-documenten in een algemeen mobiliteitsdossier of gedeelde chauffeursmap plaatsen.

26. Zaaknummering, bestandsnamen en metadata

Eenduidige metadata voorkomt verkeerde ontvangers, verwisseling van personen, dubbele dossiers en oncontroleerbare lokale bestanden.

Kernregels

- Bestandsnamen bevatten zaakcode, documenttype, datum en versie; geen onnodige naam of diagnose.
- Unieke identiteit wordt niet alleen op achternaam vastgesteld.
- Concept, definitief, vervallen en getekend zijn herkenbare statussen.
- Datum/tijd volgt één afgesproken formaat en tijdzone.

- Handmatige correcties laten de oude waarde en reden herleidbaar.

Werkinstructie

1. Gebruik het sjabloon: [ZAAKCODE]_[DOCUMENTTYPE]_[YYYYMMDD]_[VERSIE].
2. Controleer zaakcode en betrokkene vóór upload, verzending of koppeling.
3. Vul verplichte metadata in en kies classificatie/retentie.
4. Markeer vervallen documenten en blokkeer gebruik als operationele bron.
5. Voer periodieke dubbele-dossiercontrole uit.

Verplichte vastlegging

Metadata, versiehistorie, uploadlog, correctiereden en duplicaatbesluit.

Direct escaleren of stoppen

Stop verzending of uitvoering bij twijfel over identiteit, zaakcode, documentstatus of subzaak.

27. Intake, bronverificatie en gegevenskwaliteit

Informatie wordt bij intake gecontroleerd op bron, juistheid, actualiteit, bevoegdheid en volledigheid voordat zij operationele besluiten stuurt.

Kernregels

- Feiten, verklaringen, aannames en nog te verifiëren informatie zijn onderscheidbaar.
- Contactgegevens en bevoegdheid van de melder worden proportioneel gecontroleerd.
- Kritieke velden zoals locatie, voertuig, identiteit, vrijgave en ontvanger krijgen terugleescontrole.
- Correcties worden gedateerd en niet stilzwijgend overschreven.
- Onzekerheid wordt zichtbaar gemaakt in plaats van als feit opgeslagen.

Werkinstructie

1. Registreer bron, kanaal, datum/tijd en medewerker.
2. Voer terugleescontrole uit op kritieke gegevens.
3. Vraag bewijs of tweede bron wanneer risico dit vereist.
4. Markeer openstaande verificatie met eigenaar en deadline.
5. Bevestig definitieve gegevens vóór dispatch, overdracht of externe verzending.

Verplichte vastlegging

Intakelog, bronvermelding, verificatiestatus, correctielog en dispatchvrijgave.

Direct escaleren of stoppen

NO-GO bij niet-opgeloste identiteitstwijfel, verkeerde locatie, onbevoegde opdrachtgever of conflicterende EMS-vrijgave.

28. Bronregistratie en AFAS-governance

De formeel aangewezen centrale omgeving - beoogd AFAS of een gecontroleerde combinatie daarvan - is de bronregistratie voor dossiers, taken, autorisaties, documenten en status.

Kernregels

- Processen bepalen de configuratie; systeemgemak bepaalt niet de juridische of operationele noodzaak.
- E-mail en chat worden waar relevant in het zaakdossier opgenomen en daarna uit tijdelijke kanalen verwijderd.
- Lokale spreadsheets en downloads zijn alleen tijdelijk en gecontroleerd.
- Koppelingen gebruiken minimale rechten, technische accounts en logging.
- Een systeemwijziging vereist test, fallback en datamigratiecontrole.

Werkinstructie

1. Leg per gegevensobject vast welk systeem de bron is.
2. Configureer rollen, velden, workflows, logging, retentie en exportbeperkingen.
3. Test met representatieve scenario's voor Mobiliteit, EMS en COMBI.
4. Documenteer migratie, reconciliatie en foutafhandeling.
5. Voer periodiek bronregistratie- en schaduwbestandcontrole uit.

Verplichte vastlegging

Systeemarchitectuur, configuratiebesluit, testverslag, koppelingenregister, migratiebewijs en auditlog.

Direct escaleren of stoppen

Geen structureel dossierbeheer in privé-e-mail, onbeheerde cloudmap of losse lokale spreadsheet.

29. E-mail, chat, WhatsApp en telefonische informatie

Communicatiekanalen ondersteunen de uitvoering, maar worden niet automatisch als veilige of complete dossieromgeving beschouwd.

Kernregels

- Zakelijke accounts en door DriveBack beheerde apparaten zijn verplicht.
- Zeer vertrouwelijke gegevens worden via goedgekeurd beveiligd kanaal gedeeld.
- Chatgroepen hebben eigenaar, deelnemersbeheer en verwijderregels.
- Spraakmemo's en screenshots worden vermeden wanneer tekst of formeel document volstaat.
- Relevante besluiten en bewijsstukken worden tijdig in de bronregistratie vastgelegd.

Werkinstructie

1. Controleer ontvanger, zaakcode en minimale bijlage vóór verzenden.
2. Gebruik beveiligde link, encryptie of portaal voor gevoelige documenten.
3. Leg operationeel relevante communicatie vast in het dossier.
4. Verwijder tijdelijke kopieën uit downloads, chat en apparaat volgens procedure.
5. Meld verkeerde ontvanger, verloren toestel of accountmisbruik direct.

Verplichte vastlegging

Verzendlog, dossiernotitie, deel-linkinstellingen, verwijderbewijs en eventuele incidentregistratie.

Direct escaleren of stoppen

Geen ID-kopieën, medische informatie, EMS-documenten of volledige dossiers via onbeheerde WhatsApp-groep of privé-e-mail.

30. Identiteits-, reis- en voertuigdocumenten

Paspoorten, rijbewijzen, kentekenbewijzen, verzekeringsdocumenten, tickets en sleuteldocumentatie worden alleen gekopieerd of bewaard wanneer verificatie niet op een minder ingrijpende manier kan.

Kernregels

- Leg bij voorkeur verificatiestatus en noodzakelijke kenmerken vast in plaats van een volledige kopie.
- Niet-benodigde gegevens en burgerservicenummer worden afgeschermd waar wettelijk en praktisch mogelijk.
- Kopieën krijgen doel, toegang, uiterste verwijderdatum en watermerk indien passend.
- Documenten worden niet hergebruikt voor andere opdrachten zonder nieuwe noodzaak.
- Sleutel- en documentcustody is aantoonbaar.

Werkinstructie

1. Bepaal welke kenmerken nodig zijn voor de opdracht of autoriteit.
2. Verifieer live of via beveiligde upload.
3. Maak alleen indien noodzakelijk een geminimaliseerde kopie.
4. Koppel aan zaak en stel korte verwijdertermijn in.
5. Verwijder na doelbereik en controleer ook tijdelijke opslag/exports.

Verplichte vastlegging

Verificatiestatus, kopie-noodzaak, watermerk, custodylog, verwijderdatum en vernietigingsbewijs.

Direct escaleren of stoppen

Volledige identiteitskopie bewaren zonder doel, grondslag, afscherming en verwijderdatum is niet toegestaan.

31. Foto’s, video, audio en beeldregistratie

Beeld en geluid worden doelgericht, minimaal en veilig gemaakt; herkenbare personen, woningen, documenten, GPS-schermen en overledenen worden niet onnodig vastgelegd.

Kernregels

- Voertuigconditiefoto’s richten zich op schade en context, niet op privébezittingen of omstanders.
- Fotografie van een overledene is geen standaard dossierhandeling.
- Audio-opnamen vereisen vooraf vastgestelde noodzaak, informatie en bewaartermijn.
- Persoonlijke telefooncamera’s zijn niet toegestaan voor zaakbeelden.
- Metadata en geolocatie worden beoordeeld en waar nodig verwijderd.

Werkinstructie

1. Bepaal doel, noodzakelijke beelden en toegestane apparatuur.
2. Controleer omgeving op onbedoelde personen, documenten of gevoelige objecten.
3. Upload direct naar de beveiligde zaak en verifieer koppeling.
4. Verwijder lokale kopieën na gecontroleerde upload.
5. Beperk toegang en pas retentie/legal hold toe.

Verplichte vastlegging

Beeldindex, maker, datum/tijd, doel, zaakcode, uploadcontrole, toegang en verwijderdatum.

Direct escaleren of stoppen

Stop en escaleren bij verzoek om foto van een overledene, voyeuristisch beeld, heimelijke opname of gebruik voor marketing zonder aparte rechtmatige beoordeling.

32. Papieren dossiers, printen en fysieke beveiliging

Papier wordt alleen gebruikt wanneer operationeel of wettelijk nodig en wordt beschermd tegen inzage, verlies, verwisseling en ongecontroleerde vernietiging.

Kernregels

- Print alleen noodzakelijke pagina’s en haal afdrukken direct op.
- Vertrouwelijke print heeft zaakcode en classificatie, maar geen onnodige gegevens op kaft.
- Transport gebeurt in gesloten map/tas met custody.
- Bureaus, voertuigen, hotelkamers en printers zijn geen permanente opslagplaats.
- Vernietiging gebeurt via goedgekeurde vertrouwelijke afvalstroom.

Werkinstructie

1. Registreer noodzaak en aantal papieren kopieën.
2. Nummer operationele sets waar verwisseling risico geeft.
3. Bewaar in afsluitbare kast of tas en beperk sleuteltoegang.
4. Scan en verifieer terug in bronregistratie indien vereist.
5. Vernietig kopieën en registreer bij zeer vertrouwelijke stukken.

Verplichte vastlegging

Print-/uitgiftelog, custody, scancontrole en vernietigingscertificaat of -registratie.

Direct escaleren of stoppen

Geen EMS- of personeelsdossier onbeheerd in voertuig, hotel, balie, printer of open kast achterlaten.

33. Versiebeheer, correcties en audittrail

Dossierwijzigingen blijven herleidbaar zodat DriveBack kan aantonen wie wat wanneer en waarom heeft toegevoegd, gecorrigeerd, vrijgegeven of verwijderd.

Kernregels

- Definitieve documenten worden niet overschreven zonder versie of correctiespoor.
- Feitelijke fouten worden gecorrigeerd met reden en bron.
- Loggegevens worden tegen gewone gebruikerswijziging beschermd.
- Backdating en wijziging van incidenttijdlijnen zijn verboden.
- Audittrailtoegang is beperkt tot bevoegde controle- en incidentrollen.

Werkinstructie

1. Markeer documentstatus en versie.
2. Gebruik correctiefunctie of addendum in plaats van onzichtbaar overschrijven.
3. Leg naam, datum/tijd, reden en bron vast.
4. Laat kritieke wijzigingen vierogen controleren.
5. Controleer logs periodiek op ongebruikelijke wijziging of verwijdering.

Verplichte vastlegging

Versiehistorie, correctielog, autorisator, auditlog en afwijkingsonderzoek.

Direct escaleren of stoppen

Direct incidentmelding bij aanwijzing voor manipulatie, backdating, ongeautoriseerde verwijdering of loguitschakeling.

34. Delen, exporteren en beveiligde gegevensoverdracht

Gegevens worden alleen gedeeld met geverifieerde ontvangers die ze voor een rechtmatig doel nodig hebben, via een passend beveiligd kanaal.

Kernregels

- Deel altijd de minimale set en bij voorkeur via tijdgebonden toegang.
- Ontvangeridentiteit, rol en bevoegdheid worden gecontroleerd.
- Publieke links, onbeperkte doorstuurrechten en permanente downloads staan uit.
- Buitenlandse overdracht en doorgifte buiten de EER worden vooraf beoordeeld.
- Exportfuncties en bulkdownloads zijn beperkt en gelogd.

Werkinstructie

1. Verifieer ontvanger via bekend contact of tweede kanaal.
2. Controleer doel, grondslag, contract en land.
3. Redigeer of selecteer de minimale gegevensset.
4. Gebruik beveiligde verzending met vervaldatum en toegangscontrole.
5. Registreer wat, waarom, wanneer, aan wie en via welk kanaal is gedeeld.

Verplichte vastlegging

Ontvangerslog, verificatie, overdrachtsgrond, verzendbewijs, toegangslog en eventuele verwijderbevestiging.

Direct escaleren of stoppen

Stop bij last-minute gewijzigd e-mailadres, afwijkend bank-/portaalverzoek, onduidelijke buitenlandse ontvanger of druk om beveiliging over te slaan.

35. Dossierafsluiting en volledigheidscontrole

Een zaak wordt pas gesloten nadat operationele overdracht, financiële registratie, documentcontrole, openstaande acties, incidenten en retentieclassificatie zijn afgerond.

Kernregels

- Sluiting is een formele status met datum en verantwoordelijke.
- Tijdelijke kopieën en toegangsrechten worden na afsluiting ingetrokken.
- Open incidenten, claims of klachten blokkeren definitieve vernietiging.
- Onnodige ruwe data wordt verwijderd; kernbewijs blijft volgens termijn.
- EMS en COMBI krijgen vierogen-afsluitcontrole.

Werkinstructie

1. Controleer verplichte documenten, tijdlijn, overdracht en kosten.
2. Sluit open taken of zet gemotiveerd over naar beheer/claimdossier.
3. Verwijder tijdelijke bestanden, downloads, chatbijlagen en deel-links.
4. Stel retentiecategorie en eventuele legal hold vast.
5. Laat bevoegde medewerker afsluiten en registreer steekproefresultaat.

Verplichte vastlegging

Afsluitchecklist, ontbrekende-stukkenbesluit, ingetrokken rechten, verwijderlog, retentie en goedkeuring.

Direct escaleren of stoppen

Geen zaak sluiten met onbekende ontvanger, ontbrekende EMS-custody, onverklaarde datalekmelding of actieve publieke deel-link.

36. Bewaartermijnenmatrix

DriveBack stelt per gegevenscategorie een termijn vast op basis van doel, wettelijke verplichting, contract, claimrisico en proportionaliteit. De hieronder opgenomen termijnen zijn interne uitgangspunten die vóór livegang juridisch en technisch worden bekrachtigd.

Kernregels

- Er bestaat geen algemene regel dat elk operationeel dossier zeven jaar moet worden bewaard.
- Fiscale bewaarplicht geldt voor de fiscale basisadministratie, niet automatisch voor alle foto’s, GPS-routes of medische informatie.
- Korte termijn is de standaard voor ruwe tracking, opnamen en identiteitskopieën.

- Claims, onderzoeken en wettelijke bevelen kunnen via legal hold verlengen.
- Automatische verwijdering wordt getest en steekproefsgewijs gecontroleerd.

Werkinstructie

1. Koppel iedere dataset aan doel, startmoment, termijn en trigger.
2. Laat juridisch/fiscaal beoordelen waar wettelijke of contractuele termijnen spelen.
3. Configureer waarschuwing, archivering en verwijdering.
4. Blokkeer verwijdering alleen via geregistreerde legal hold.
5. Controleer maandelijks uitzonderingen en jaarlijks de matrix.

Verplichte vastlegging

Bewaarmatrix, juridische validatie, systeemconfiguratie, verwijderlog, uitzonderingen en reviewverslag.

Direct escaleren of stoppen

Geen permanente bewaring “voor het geval dat”; iedere verlenging heeft concrete reden, eigenaar en eindbeoordeling.

Interne bewaartermijnen - te bekrachtigen

Gegevenscategorie	Uitgangstermijn	Doel	Opmerking
Mobiliteitszaak: kernopdracht, overdracht, communicatiebewijs	2 jaar na sluiting	Contract/claim/kwaliteitsbewijs	5 jaar bij actieve claim of legal hold
EMS-zaak: kernopdracht, vrijgave, custody, overdracht	2 jaar na overdracht, daarna review	Bewijs, waardigheid, claimbeheersing	Langer alleen na juridische validatie of legal hold
Voertuigconditiefoto’s	2 jaar na sluiting	Schade- en overdrachtsbewijs	5 jaar bij claim/legal hold
Ruwe GPS-routehistorie	90 dagen na rit	Veiligheid, dispatch, incidentanalyse	Korter waar systeem dit veilig ondersteunt
GPS-mijlpalen/check-ins in zaak	2 jaar na sluiting	Aantoonbare uitvoering en veiligheid	Geen continue route bewaren als mijlpalen volstaan
Gespreksopnamen	90 dagen	Kwaliteit, bewijs, incidentonderzoek	Langer alleen gemotiveerd geselecteerd fragment
Dashcam/camerabeelden	Maximaal 28 dagen	Veiligheid/incident	Direct veiligstellen bij incident of claim
ID-/reisdocumentkopieën	Na doelbereik, uiterlijk 30 dagen	Verificatie/reisuitvoering	Langer alleen concrete wettelijke/contractuele noodzaak
Gezondheids-/uitvalbewijs klant	Na doelbereik, uiterlijk 6 maanden	Aantoonbare uitval/claim	Minimaliseren; diagnose vermijden
Privacyverzoeken en besluit	3 jaar na afsluiting	Verantwoordingsplicht en geschil	Legal hold indien procedure loopt
Datalekregister en incidentdossier	5 jaar na afsluiting	Verantwoordingsplicht, trendanalyse	Ernstige incidenten volgens juridische review
Normale beveiligingslogs	12 maanden	Detectie en onderzoek	Afhankelijk van risico en systeemcapaciteit
Beheer-/privileged logs	24 maanden	Misbruik- en integriteitsonderzoek	Streng beperkt en gemonitord
Leveranciers-/verwerkersdossier	7 jaar na einde contract	Contract- en verantwoordingsbewijs	Selectieve verwijdering van overbodige persoonsgegevens
Fiscale basisadministratie	7 jaar	Fiscale bewaarplicht	Specifieke fiscale uitzonderingen apart toetsen
Afgewezen sollicitanten	4 weken na einde procedure	Werving	Tot 1 jaar met geldige toestemming
Algemeen personeelsdossier	2 jaar na einde dienstverband	Werkgeversadministratie/claim	Specifieke loon/fiscale stukken langer
Back-upkopieën	Rollend [IN TE VULLEN; beoogd 35 dagen]	Herstel	Verwijdering door rotatie; legal hold niet via gewone back-up

37. Legal hold, archivering en vernietiging

Verwijdering wordt tijdelijk geblokkeerd wanneer concrete claims, onderzoeken, klachten, incidenten of wettelijke bevelen dit vereisen; een legal hold is nauwkeurig en niet breder of langer dan nodig.

Kernregels

- Legal hold wordt schriftelijk geopend door bevoegde juridische/directierol.
- Betrokken systemen, dossiers, logs en bewaareigenaren zijn benoemd.
- Gewone gebruikers kunnen een hold niet opheffen.
- Periodieke review voorkomt onbeperkte bewaring.
- Na opheffing hervat de normale termijn en volgt gecontroleerde vernietiging.

Werkinstructie

1. Registreer aanleiding, scope, startdatum, eigenaar en juridische basis.
2. Identificeer alle relevante locaties, exports, e-mail en leveranciers.
3. Blokkeer automatische verwijdering en informeer noodzakelijke beheerders.
4. Review minimaal per kwartaal en na relevante gebeurtenis.
5. Hef schriftelijk op, voer verwijdering uit en bewaar bewijs.

Verplichte vastlegging

Legal-holdregister, technische blokkering, notificaties, review, opheffing en vernietigingsbewijs.

Direct escaleren of stoppen

Een informele opmerking “bewaar alles maar” is geen geldige legal hold en wordt geëscaleerd.

38. Verwijderen, anonimiseren en back-uprotatie

Verwijdering omvat actieve systemen, lokale kopieën, deel-links, apparaten, exports en waar mogelijk leveranciersomgevingen; anonimisering is alleen geldig wanneer heridentificatie redelijkerwijs niet meer mogelijk is.

Kernregels

- Verwijderen uit een gebruikersscherm is niet automatisch technische vernietiging.
- Back-ups volgen vaste rotatie en worden niet handmatig aangepast zonder herstelrisicoanalyse.
- Pseudonimisering is geen anonimisering en blijft AVG-verwerking.
- Vernietiging van zeer vertrouwelijke papier- en datadragers is aantoonbaar.
- Restdata en zoekindexen worden meegenomen in technische test.

Werkinstructie

1. Bepaal scope en controleer legal hold.
2. Voer verwijdering of aantoonbare anonimisering uit in bron en afgeleide locaties.
3. Laat back-upkopieën via gedocumenteerde rotatie verlopen.
4. Test steekproefsgewijs zoeken, herstel en heridentificatie.
5. Registreer resultaat, afwijkingen en corrigerende actie.

Verplichte vastlegging

Verwijderopdracht, systeemlog, leveranciersbevestiging, back-uprotatie, anonimiseringstest en vernietigingscertificaat.

Direct escaleren of stoppen

Geen “anonimiseren” claimen wanneer zaakcode, route, datum, voertuig of familiecontext de persoon nog herkenbaar maakt.

DEEL IV

AUTORISATIES EN INFORMATIEBEVEILIGING

Least privilege, JML, MFA, apparaten, netwerk, leveranciers, logging en continuïteit

39. Role-Based Access Control en least privilege

Toegang wordt verleend op basis van formele functie, taak, zaakbetrokkenheid en minimale noodzakelijkheid. Brede toegang voor gemak is niet toegestaan.

Kernregels

- Rollen zijn vooraf gedefinieerd en gekoppeld aan processen en gegevensclassificaties.
- Zaaktoegang is waar mogelijk tijdelijk en automatisch gekoppeld aan opdrachtstatus.
- EMS, HR, incidentonderzoek, financiën en systeembeheer hebben afzonderlijke rollen.
- Lees-, wijzig-, export-, verwijder- en beheierrechten worden apart beoordeeld.
- Uitzonderingen zijn tijdelijk, gelogd en door twee bevoegde personen goedgekeurd.

Werkinstructie

1. Bepaal de minimale taken per rol.
2. Koppel rol aan systemen, modules, dossiercategorieën en acties.
3. Test met een standaardaccount en negatief scenario.
4. Laat leidinggevende én informatie-eigenaar toegang goedkeuren.
5. Herbeoordeel bij functiewijziging, incident en minimaal halfjaarlijks.

Verplichte vastlegging

Rollenmatrix, aanvraag, goedkeuring, technische toekenning, testbewijs, review en intrekking.

Direct escaleren of stoppen

Geen gedeelde “algemene” accounts en geen toegang tot alle EMS- of personeelsdossiers vanwege senioriteit.

40. Autorisatiematrix per functie en dienststroom

De autorisatiematrix maakt concreet welke functie welke gegevens mag zien of bewerken en vormt de basis voor systeemconfiguratie en audits.

Kernregels

- Directie heeft bestuurlijke inzage, maar medische en operationele details alleen bij taaknoodzaak.
- Meldkamer/planning ziet intake, dispatch, veiligheid en contactgegevens.
- Chauffeurs zien een beperkte uitvoeringsset en geen volledige financiële of historische dossiers.
- EMS-crews zien uitsluitend de EMS-opdracht, custody, veiligheidsinformatie en ontvanger.
- Administratie, HR, IT en externe adviseurs hebben gescheiden domeinrechten.

Werkinstructie

1. Stel per rol Read, Create, Update, Export, Delete en Admin vast.
2. Markeer ZEER VERTROUWELIJK en vierogenhandelingen.
3. Configureer systemen en voer gebruikersacceptatietest uit.
4. Laat afwijkingen expliciet goedkeuren.
5. Vergelijk matrix en werkelijkheid in iedere toegangsreview.

Verplichte vastlegging

Goedgekeurde autorisatiematrix, systeemexport van rechten, testverslag, uitzonderingen en review.

Direct escaleren of stoppen

Wanneer het systeem de benodigde functiescheiding niet ondersteunt, volgt aanvullende maatregel of NO-GO voor de betreffende verwerking.

Basismatrix - te vertalen naar technische systeemrollen

Rol	Mobiliteit	EMS	HR	Beperkingen
Directie	Samenvatting, risico, contract, incidentbesluit	Alleen taakgericht	Geen standaard medische details	Geen dagelijks beheer
Meldkamer / Planning	R/W actuele DBM-zaken	R/W actuele EMS-intake voor toegewezen team	Beperkte operationele inzetinformatie	Geen beheer
DriveBack-chauffeur	R toegewezen opdracht; upload foto/rapport	Geen toegang behalve COMBI-minimum	Eigen documenten/rooster	Geen export/bulk
EMS-crew	Alleen COMBI-minimum indien nodig	R/W toegewezen EMS-uitvoering en custody	Eigen documenten/rooster	Geen bulk/export buiten taak
Administratie	Factuur- en kostenreferenties	Factuur- en kostenreferenties	Loon/fiscaal volgens rol	Geen operationele beeldset
HR	Geen zaakinhoud	Geen zaakinhoud	R/W personeelsdossier; geen bedrijfsartsdossier	Geen operationele dossiers
Privacycoördinator / FG	Inzage voor toezicht/verzoek/incident	Idem, met strikte logging	Noodzakelijke privacy-inzage	Geen operationele besluitvorming
IT-beheer	Metadata en techniek	Metadata en techniek	Metadata en techniek	Inhoud alleen na ticket/noodzaak
Externe verwerker	Volgens contract en instructie	Volgens contract en instructie	Volgens contract en instructie	Tijdelijk, gelogd, minimaal

41. Joiner-Mover-Leaverproces

Toegang volgt de actuele arbeids- of opdrachtrelatie. Instroom, functiewijziging en uitdiensttreding worden tijdig, volledig en controleerbaar verwerkt.

Kernregels

- Geen account vóór geverifieerde identiteit, contract, functie en goedkeuring.
- Standaardrol is minimaal; extra rechten worden apart aangevraagd.
- Functiewijziging trekt oude rechten eerst in voordat nieuwe rechten actief worden.
- Bij uitdiensttreding of risico wordt toegang uiterlijk op het afgesproken moment geblokkeerd.
- Apparaten, sleutels, tokens, passen, exports en gedeelde geheimen worden teruggenomen of gewijzigd.

Werkinstructie

1. HR of opdrachtgever start een JML-ticket met effectieve datum en rol.
2. Leidinggevende en informatie-eigenaar keuren rechten goed.
3. IT voert aanmaak, wijziging of blokkering uit en bevestigt.
4. Controleer mailbox, groepen, API-tokens, voertuigapps, VPN, portals en fysieke toegang.
5. Laat onafhankelijke controle uitvoeren en archiveer bewijs.

Verplichte vastlegging

JML-formulier, goedkeuring, accountlijst, apparaat-/sleutelinname, blokkeringstijd en controle.

Direct escaleren of stoppen

Directe blokkering bij ontslag op staande voet, vermissing apparaat, integriteitsincident of onbevoegde gegevensdownload.

42. Identiteit, wachtwoorden en MFA

Iedere gebruiker heeft een persoonlijk account. Sterke authenticatie en MFA beschermen cloud, e-mail, dossier, VPN, beheer en externe toegang.

Kernregels

- Gedeelde accounts zijn verboden, behalve strikt technische serviceaccounts met eigenaar en kluisbeheer.
- Wachtwoorden zijn uniek, lang en worden niet via e-mail of chat gedeeld.
- MFA gebruikt bij voorkeur phishingresistente methode voor beheer en kritieke systemen.
- Herstelcodes en noodtokens worden als ZEER VERTROUWELIJK beheerd.
- Inlogpogingen, MFA-wijzigingen en herstelacties worden gelogd.

Werkinstructie

1. Verifieer identiteit vóór uitgifte of reset.
2. Activeer persoonlijk account met minimale rol en MFA.
3. Bewaar geheimen in goedgekeurde wachtwoordmanager.
4. Review mislukte logins, ongebruikelijke locaties en MFA-reset.
5. Blokkeer en reset bij twijfel; onderzoek sessies en tokens.

Verplichte vastlegging

Accountregistratie, MFA-status, resetlog, herstelcodescustody en beveiligingswaarschuwingen.

Direct escaleren of stoppen

Geen telefonische wachtwoordreset op basis van naam of functie alleen; gebruik vaste verificatieprocedure.

43. Beheerdersrechten en break-glassaccounts

Beheerdersrechten worden beperkt tot afzonderlijke beheeraccounts en uitsluitend gebruikt voor beheertaken. Noodtoegang is verzegeld, gelogd en achteraf gecontroleerd.

Kernregels

- Dagelijks e-mailen of browsen met beheeraccount is verboden.
- Privileged access is tijdelijk waar de techniek dit ondersteunt.
- Break-glassaccounts hebben sterke unieke authenticatie en tweepersoonsbeheer.
- Gebruik genereert directe melding aan een onafhankelijke reviewer.
- Leveranciersbeheer is tijdgebonden en alleen na ticket.

Werkinstructie

1. Maak separate beheeridentiteiten en wijs eigenaar toe.
2. Beperk systemen, acties en tijdvenster.
3. Registreer ticket, doel, start en verwachte eindtijd.
4. Controleer logs en wijzigingen na afloop.
5. Trek rechten in, roteer geheimen en sluit ticket.

Verplichte vastlegging

Privileged-accessregister, ticket, sessielog, change, review en sleutelrotatie.

Direct escaleren of stoppen

Onverklaard gebruik van beheer- of break-glassaccount is een kritisch beveiligingsincident.

44. Toegangsreviews en logging van inzage

DriveBack controleert periodiek of actieve accounts, rollen en dossierinzage nog passen bij functie en taak.

Kernregels

- Kritieke en externe toegang wordt minimaal per kwartaal beoordeeld.
- Overige rollen worden minimaal halfjaarlijks beoordeeld.
- Inactieve accounts, brede groepsrechten en onbekende serviceaccounts worden onderzocht.
- EMS-, HR- en incidentdossierinzage wordt steekproefsgewijs op noodzaak gecontroleerd.
- Review wordt uitgevoerd door iemand anders dan de technische uitvoerder.

Werkinstructie

1. Exporteer actuele accounts, rollen, groepen, laatste login en uitzonderingen.
2. Laat leidinggevende en informatie-eigenaar bevestigen of intrekken.
3. Controleer afwijkende inzage en bulkexports.
4. Voer correcties uit binnen vastgestelde termijn.
5. Registreer bevindingen, bewijs en verbeteracties.

Verplichte vastlegging

Rechtenexport, reviewbesluit, intrekkingslog, inzageanalyse, afwijkingen en CAPA.

Direct escaleren of stoppen

Direct escaleren bij ex-medewerkeraccount, onbekende beheerder, bulkexport zonder taak of herhaalde inzage in niet-toegewezen EMS-zaken.

45. Vertrouwelijkheid, clean desk en functiescheiding

Menselijk gedrag is onderdeel van beveiliging. Gesprekken, schermen, prints, sleutels en documenten worden beschermd tegen onbevoegde waarneming en vermenging.

Kernregels

- Medewerkers ondertekenen geheimhouding en krijgen rolgerichte instructie.
- Schermvergrendeling is verplicht bij verlaten werkplek.
- Whiteboards, notities en dienstoverdracht bevatten minimale persoonsgegevens.
- Bezoekers worden begeleid en hebben geen zicht op meldkamer- of EMS-informatie.
- Fraudegevoelige acties zoals bankrekeningwijziging, bulkexport en verwijdering vereisen vierogencontrole.

Werkinstructie

1. Controleer werkplek aan begin en einde dienst.
2. Gebruik privacyfilters en afgeschermde gespreksruimte waar nodig.
3. Berg papier, tokens en sleutels afsluitbaar op.
4. Verifieer gevoelige wijzigingen via tweede kanaal.
5. Meld overtreding of bijna-incident zonder uitstel.

Verplichte vastlegging

Geheimhoudingsverklaring, werkplekinspectie, bezoekerslog, vierogenbewijs en incidentmelding.

Direct escaleren of stoppen

Geen dossierbespreking in lift, restaurant, openbaar vervoer of gedeelde hotelruimte.

46. Mobiele apparaten, MDM en BYOD

Smartphones, tablets en laptops die DriveBack-gegevens verwerken zijn beheerd, versleuteld, updatebaar en op afstand blokkeerbaar.

Kernregels

- Zakelijke apparaten zijn de standaard voor operationeel werk.
- BYOD is alleen toegestaan na expliciete risicoacceptatie, containerisering en technische beheersing.
- Schijfversleuteling, schermvergrendeling, MDM, updatebeleid en malwarebescherming zijn verplicht.
- Lokale opslag en offline bestanden worden geminimaliseerd.
- Rooted/jailbroken of niet-ondersteunde apparaten zijn verboden.

Werkinstructie

1. Registreer apparaat, eigenaar, serienummer, gebruiker en classificatie.
2. Installeer MDM, versleuteling, certificaten, zakelijke apps en remote wipe.
3. Test blokkering, updates, back-up en gegevensscheiding.
4. Monitor compliance en blokkeer niet-conforme apparaten.
5. Wis en neem in bij einde gebruik of incident.

Verplichte vastlegging

Assetregister, MDM-status, compliance, uitgifte/inname, remote-wipetest en incidentlog.

Direct escaleren of stoppen

Vermist apparaat, uitgeschakelde MDM, ontbrekende encryptie of privé-back-up van zaakgegevens is direct meldplichtig intern.

47. Thuiswerken, reizen en externe toegang

Externe toegang ondersteunt continuïteit, maar vereist een vertrouwde identiteit, beheerd apparaat, veilige verbinding en afgeschermde werkomgeving.

Kernregels

- VPN of door DriveBack goedgekeurde beveiligde toegang is verplicht waar van toepassing.
- Openbare WiFi wordt vermeden of uitsluitend via beschermde verbinding gebruikt.
- Schermen en gesprekken zijn afgeschermd van huisgenoten, medereizigers en hotelpersoneel.
- Documenten worden niet op hotelprinter of publieke businesscentercomputer verwerkt.
- Hoge-risicolanden en grensinspecties krijgen voorafgaande reisbeveiligingsinstructie.

Werkinstructie

1. Controleer apparaatcompliance, MFA en verbinding vóór toegang.
2. Gebruik minimale offline opdrachtset.
3. Werk in afsluitbare, private ruimte en vergrendel bij onderbreking.
4. Meld grenscontrole, inbeslagname, ongebruikelijke prompt of verlies direct.
5. Synchroniseer, verwijder tijdelijke data en sluit sessies na inzet.

Verplichte vastlegging

Externe-toegangslog, reisrisicobeoordeling, uitgegeven apparatuur, incident en verwijdercontrole.

Direct escaleren of stoppen

Geen toegang tot EMS- of HR-dossiers vanaf onbeheerde gedeelde computer of zichtbaar in openbare ruimte.

48. Assetregister en informatie-eigenaarschap

DriveBack onderhoudt een actueel register van hardware, software, cloudservices, voertuigtelematica, koppelingen, dataopslag, papieren archieven en kritieke leveranciers.

Kernregels

- Ieder asset heeft bedrijfs- en technisch eigenaar, classificatie, locatie en levenscyclusstatus.
- Onbekende software of account wordt onderzocht en waar nodig verwijderd.
- Licenties, ondersteuning en end-of-life worden bewaakt.
- Afvoer van apparaten omvat veilige datavernietiging.
- Kritieke afhankelijkheden en single points of failure zijn zichtbaar.

Werkinstructie

1. Inventariseer en label alle assets en diensten.
2. Koppel data, proces, eigenaar, leverancier, contract en risico.
3. Controleer maandelijks nieuwe/afgevoerde assets en minimaal jaarlijks volledige inventaris.
4. Plan vervanging vóór end-of-support.
5. Archiveer vernietigings- of overdrachtsbewijs.

Verplichte vastlegging

Assetregister, eigenaarschap, lifecycle, patchstatus, contract, vernietiging en risico.

Direct escaleren of stoppen

Geen operationeel systeem of GPS-apparaat zonder bekende eigenaar, leverancier, updatepad en incidentcontact.

49. Hardening, patching en kwetsbaarheden

Systemen worden veilig geconfigureerd, tijdig geüpdatet en gecontroleerd op bekende kwetsbaarheden.

Kernregels

- Onnodige diensten, standaardaccounts en open poorten worden uitgeschakeld.
- Kritieke beveiligingsupdates krijgen versnelde behandeling op basis van actuele dreiging.
- Patchuitstel heeft eigenaar, reden, compensatie en einddatum.
- Kwetsbaarheidsscans en leveranciersmeldingen worden opgevolgd.
- Productiesystemen worden getest zonder onnodige echte persoonsgegevens.

Werkinstructie

1. Onderhoud ondersteunde versies en configuratiebaseline.
2. Ontvang en beoordeel kwetsbaarheids- en patchinformatie.
3. Prioriteer op exploitatie, blootstelling, data en bedrijfsimpact.
4. Test, implementeer en verifieer; leg uitstel vast.
5. Scan opnieuw en rapporteer openstaande risico’s.

Verplichte vastlegging

Baseline, patchregister, kwetsbaarheden, uitzonderingen, implementatie- en verificatiebewijs.

Direct escaleren of stoppen

Kritiek actief misbruikbare kwetsbaarheid op internettoegankelijk systeem vereist directe containment en incidentbeoordeling.

50. Netwerk, WiFi, segmentatie en externe koppelingen

Netwerken worden gesegmenteerd zodat werkplekken, gasttoegang, voertuigtelematica, beheer, printers en kritieke systemen elkaar niet onbeperkt kunnen bereiken.

Kernregels

- Gast-WiFi is gescheiden van bedrijfsnetwerk.
- Beheerinterfaces zijn niet publiek bereikbaar zonder sterke beveiliging.
- Firewallregels zijn minimaal, gedocumenteerd en periodiek gereviewd.
- Koppelingen gebruiken versleutelde protocollen en unieke credentials.
- Ongebruikte VPN- en partnerverbindingen worden ingetrokken.

Werkinstructie

1. Maak netwerk- en datastroomdiagram.
2. Definieer zones, toegestane stromen en beheerpaden.
3. Configureer firewall, detectie, DNS-/webfiltering en veilige WiFi.
4. Test segmentatie en ongeautoriseerde route.
5. Review regels minimaal halfjaarlijks en na wijziging.

Verplichte vastlegging

Netwerkdiagram, firewallregels, testverslag, verbindingseigenaar, review en afwijkingen.

Direct escaleren of stoppen

Direct blokkeren bij onbekende externe tunnel, onbeveiligde beheerpoort of voertuig-/GPS-systeem dat brede toegang tot bedrijfsnetwerk heeft.

51. Encryptie en sleutelbeheer

Gevoelige informatie wordt passend versleuteld tijdens opslag en transport. Sleutels, certificaten en herstelcodes worden centraal en gecontroleerd beheerd.

Kernregels

- TLS en moderne beveiligde protocollen zijn standaard voor gegevensoverdracht.
- Laptops en mobiele apparaten gebruiken volledige-schijfversleuteling.
- Zeer vertrouwelijke exports krijgen aanvullende bescherming.
- Sleutels staan niet samen met versleutelde bestanden in dezelfde onbeheerde locatie.
- Rotatie, intrekking, back-up en noodherstel zijn vastgelegd.

Werkinstructie

1. Classificeer data en bepaal encryptie-eis.
2. Selecteer goedgekeurde algoritmen en sleutelopslag.
3. Wijs sleutelbeheerder en vervanger aan.
4. Monitor vervaldatum, misbruik en certificaatwijziging.
5. Roteer of trek onmiddellijk in bij incident of rolwijziging.

Verplichte vastlegging

Encryptiestandaard, sleutelregister, certificaten, rotatie, intrekking en hersteltest.

Direct escaleren of stoppen

Verstuur wachtwoord en versleuteld bestand nooit via hetzelfde kanaal zonder aanvullende bescherming.

52. E-mailbeveiliging, phishing en betalingsfraude

E-mail is een belangrijk aanvalskanaal. DriveBack combineert technische filters, MFA, verificatieprocedures en meldcultuur.

Kernregels

- Domeinbeveiliging en anti-spoofing worden technisch ingericht.
- Onverwachte bijlagen, inloglinks en verzoeken om spoed worden geverifieerd.
- Bankrekening-, wachtwoord-, MFA- en betaalwijzigingen vereisen tweede kanaal en vierogencontrole.
- Medewerkers melden verdachte berichten via één herkenbare route.
- Klikken of invoeren wordt zonder schuldvertraging direct gemeld.

Werkinstructie

1. Controleer afzender, domein, context en verzoek.
2. Open niet; verifieer via bekend telefoonnummer of portaal.
3. Meld en isoleer verdacht bericht.
4. Bij klik/invoer: verbreek waar nodig verbinding, wijzig credentials en start incidentrespons.
5. Onderzoek ontvangers, mailboxregels, tokens en betalingen.

Verplichte vastlegging

Phishingmelding, analyse, accountacties, mailboxaudit, betalingscontrole en lessons learned.

Direct escaleren of stoppen

Direct kritieke escalatie bij afwijkend bankrekeningnummer, directieverzoek tot geheimhouding, MFA-promptbombing of mailboxregel die berichten doorstuurt.

53. Cloud, SaaS, AFAS en leveranciersbeheer

Cloud- en SaaS-diensten worden alleen gebruikt na beoordeling van privacyrol, beveiliging, locatie, subverwerkers, continuïteit, exit en incidentmelding.

Kernregels

- Contract, verwerkersovereenkomst en beveiligingsbijlage sluiten aan op werkelijke dienst.
- Toegang, MFA, logging, retentie en export worden door DriveBack geconfigureerd en getest.
- Leverancierscertificaten zijn ondersteunend bewijs, geen vervanging voor eigen beoordeling.
- Subverwerkers en internationale doorgiften zijn inzichtelijk.
- Exitplan voorkomt vendor lock-in en verlies van dossierbeschikbaarheid.

Werkinstructie

1. Voer due diligence uit op organisatie, dienst, hosting, beveiliging, support en incidenthistorie.
2. Beoordeel AVG-rol, DPA, subverwerkers, doorgifte en auditrechten.
3. Test configuratie, rollen, logs, back-up, export en verwijdering.
4. Monitor SLA, kwetsbaarheden, wijzigingen en incidenten.
5. Oefen exit/export en leg alternatieve werkroute vast.

Verplichte vastlegging

Leveranciersdossier, DPA, TOMs, subverwerkerslijst, risico, acceptatie, monitoring en exit-test.

Direct escaleren of stoppen

Geen upload van echte DriveBack- of EMS-data naar proefaccount of nieuwe SaaS zonder voorafgaande goedkeuring.

54. Leveranciers, verwerkers en ketenpartners

Iedere externe partij krijgt alleen de gegevens en toegang die nodig zijn. Rollen, instructies, beveiliging, datalekmelding, subverwerking en beëindiging zijn contractueel en operationeel geregeld.

Kernregels

- Een verwerker handelt uitsluitend op gedocumenteerde instructie.
- Zelfstandige ketenpartners ontvangen gegevens op eigen grondslag en via gegevensdelingsafspraak waar passend.
- Datalekken worden zonder onredelijke vertraging aan DriveBack gemeld.
- Toegang is persoonlijk, tijdelijk en intrekbaar.
- DriveBack kan bewijs, audits of assurance opvragen passend bij risico.

Werkinstructie

1. Classificeer privacyrol en gegevensstroom.
2. Beoordeel beveiliging, continuïteit, landen, subverwerkers en incidentroute.
3. Sluit passende overeenkomst vóór gegevensdeling.
4. Onboard accounts, instructies en contactpersonen.
5. Evalueer jaarlijks en bij incident of contractwijziging; voer gecontroleerde offboarding uit.

Verplichte vastlegging

Rolbeoordeling, contract/DPA, TOMs, contactmatrix, accounts, evaluatie, incidenten en exitbevestiging.

Direct escaleren of stoppen

Geen partnerselectie uitsluitend op snelheid of prijs wanneer deze toegang krijgt tot ID-, gezondheids-, GPS- of EMS-gegevens.

55. Internationale doorgifte en buitenlandse toegang

Toegang of opslag buiten de EER wordt vooraf juridisch en technisch beoordeeld, ook wanneer een leverancier vanuit de EER wordt gebruikt maar ondersteuning elders plaatsvindt.

Kernregels

- Bepaal waar data wordt opgeslagen, gekopieerd, beheerd en ondersteund.
- Adequaatheidsbesluit, modelcontracten of andere doorgiftemechanismen worden correct toegepast.
- Aanvullende maatregelen en transfer impact assessment worden waar nodig uitgevoerd.
- Buitenlandse partner ontvangt alleen minimale opdrachtgegevens.
- Spoed heft doorgifteregels niet op; gebruik vooraf goedgekeurde landen- en partnerroute.

Werkinstructie

1. Identificeer land, ontvanger, rol, data en toegangsvorm.
2. Bepaal geldig doorgiftemechanisme en lokale risico’s.
3. Voer TIA en aanvullende technische/contractuele maatregelen uit waar nodig.
4. Informeer betrokkenen en werk register/contracten bij.
5. Monitor juridische wijziging en beëindig onrechtmatige toegang.

Verplichte vastlegging

Doorgifteregister, SCC/adequaatheid, TIA, aanvullende maatregelen, ontvangerslog en review.

Direct escaleren of stoppen

Geen ad-hoc verzending van volledig EMS- of ID-dossier naar onbekende buitenlandse mailbox onder tijdsdruk.

56. Back-up, herstel en continuïteit

Beschikbaarheid vereist versleutelde, gescheiden en geteste back-ups én een werkbare handmatige fallback voor 24/7 intake, planning en custody.

Kernregels

- Back-upfrequentie volgt RPO; herstelprioriteit volgt RTO.
- Minimaal één kopie is logisch of fysiek gescheiden van productie en ransomwarebereik.
- Back-ups zijn versleuteld en toegang is beperkt.
- Herstel wordt periodiek end-to-end getest, inclusief rechten en integriteit.
- Papieren/noodregistratie wordt achteraf gecontroleerd in bronregistratie verwerkt.

Werkinstructie

1. Bepaal kritieke processen, RPO, RTO en afhankelijkheden.
2. Configureer back-up, retentie, monitoring en mislukte-back-upmelding.
3. Test minimaal per kwartaal kritieke herstelset en jaarlijks volledige scenario's.
4. Oefen systeemuitval met handmatige intake en later reconciliëren.
5. Rapporteer resultaat en sluit tekortkomingen via CAPA.

Verplichte vastlegging

Back-upbeleid, jobs, meldingen, hersteltest, RPO/RTO-resultaat, fallbackformulieren en CAPA.

Direct escaleren of stoppen

Een succesvolle back-upmelding zonder aantoonbare hersteltest geldt niet als voldoende beschikbaarheidsmaatregel.

57. Logging, monitoring en detectie

DriveBack registreert voldoende beveiligings- en systeemgebeurtenissen om misbruik, fouten en incidenten te detecteren en reconstrueren, zonder onnodige personeelsmonitoring.

Kernregels

- Kritieke logs omvatten login, MFA, rechten, exports, delen, verwijdering, beheerwijziging en toegang tot zeer vertrouwelijke dossiers.
- Tijdbronnen zijn gesynchroniseerd.
- Logs zijn beschermd tegen wijziging en hebben passende retentie.
- Waarschuwingen hebben eigenaar, prioriteit en opvolgtermijn.
- Monitoringdoelen zijn transparant en worden niet sluipend uitgebreid.

Werkinstructie

1. Bepaal welke gebeurtenissen per systeem nodig zijn.
2. Centraliseer waar passend en bescherm logtoegang.
3. Configureer detectieregels voor bulkexport, ongebruikelijke login, beheerwijziging en mislukte toegang.
4. Onderzoek alerts volgens incidentprocedure.
5. Review dekking, ruis, retentie en privacy minimaal halfjaarlijks.

Verplichte vastlegging

Loggingmatrix, configuratie, alerts, onderzoek, review en wijzigingsbesluit.

Direct escaleren of stoppen

Geen heimelijke inhoudsmonitoring van medewerkers zonder specifieke noodzaak, grondslag, transparantie en medezeggenschapsbeoordeling.

58. AI, automatisering en geautomatiseerde besluitvorming

Generatieve AI, transcriptie, route-optimalisatie en automatische classificatie mogen alleen worden gebruikt na beoordeling van gegevensgebruik, leverancier, modeltraining, menselijk toezicht en foutenimpact.

Kernregels

- Geen persoonsgegevens of bedrijfsgeheimen in publieke AI-dienst zonder formele goedkeuring en passende overeenkomst.
- AI-output is concept en wordt door bevoegde medewerker gecontroleerd.
- Hoog-risicobesluiten over personeel, toegang, ziekte, EMS-identiteit of opdrachtacceptatie worden niet blind geautomatiseerd.
- Prompts, uploads en output volgen dossier- en retentieregels.
- Modelwijzigingen en leverancierstraining op DriveBack-data staan standaard uit.

Werkinstructie

1. Registreer use case, doel, data, leverancier en beslisimpact.
2. Voer privacy-, security- en waar nodig AI-/DPIA-beoordeling uit.
3. Configureer geen-training, logging, toegang en retentie.
4. Test fouten, bias, hallucinaties, uitlegbaarheid en fallback.
5. Laat mens beslissen en evalueer periodiek.

Verplichte vastlegging

AI-register, beoordeling, contract, configuratie, test, menselijk besluit en incidenten.

Direct escaleren of stoppen

Geen invoer van EMS-documenten, paspoorten, medische informatie of volledige dossiers in niet-goedgekeurde AI-tool.

DEEL V

INCIDENTEN EN DATALEKKEN

Melden, triage, containment, 72-uursbeoordeling, communicatie en herstel

59. Incidenttaxonomie en meldcultuur

Iedere gebeurtenis die beschikbaarheid, vertrouwelijkheid, integriteit, privacy, fysieke documentbeveiliging of operationele continuïteit kan raken, wordt laagdrempelig en direct gemeld.

Kernregels

- Een incident hoeft nog geen bewezen datalek te zijn om gemeld te worden.
- Bijna-incidenten worden geregistreerd om herhaling te voorkomen.
- Melden te goeder trouw leidt niet tot benadeling; verzwijgen of bewijs wissen is ernstig.
- Cyber-, privacy-, fysieke-, leveranciers- en operationele incidenten gebruiken één ingang.
- De incidentleider bepaalt verdere classificatie, niet de melder alleen.

Werkinstructie

1. Stop de onveilige handeling zonder bewijs te vernietigen.
2. Bel het interne 24/7-incidentnummer [IN TE VULLEN] bij urgentie.
3. Registreer wat, wanneer, waar, wie, welk systeem/dossier en eerste impact.
4. Volg instructies voor containment en bereikbaarheid.
5. Werk mee aan feitenonderzoek en leermaatregelen.

Verplichte vastlegging

Incidentmelding, tijdlijn, melder, betrokken assets/data, eerste maatregelen en classificatie.

Direct escaleren of stoppen

Direct telefonisch melden bij actieve aanval, verkeerde EMS-identiteit, onbevoegde dossierinzage, verloren apparaat, ransomware, systeemuitval of externe publicatie.

60. Eerste 30 minuten en incidentleiding

De eerste reactie richt zich op veiligheid, behoud van bewijs, beperking van schade, continuïteit en snelle vaststelling van verantwoordelijkheden.

Kernregels

- Incidentleider, technisch leider, privacybeoordelaar, proceseigenaar en communicatieverantwoordelijke worden benoemd.
- Eén tijdlijn en één feitenbron voorkomen tegenstrijdige informatie.
- Containment wordt afgewogen tegen bewijs en continuïteit.
- Alle externe communicatie loopt via bevoegde woordvoering.
- Aannames worden als aannames gemarkeerd.

Werkinstructie

1. Bevestig melding en open uniek incidentnummer.
2. Bepaal directe veiligheid en of systemen/accounts geïsoleerd moeten worden.
3. Benoem incidentleider en kernteam.
4. Beveilig logs, berichten, apparatuur en relevante dossierkopie.
5. Plan eerste beslismoment binnen 30 minuten en volgende update.

Verplichte vastlegging

Incidentnummer, rolverdeling, tijdlijn, containmentbesluit, bewijsregister en updatecadans.

Direct escaleren of stoppen

Geen fabriekreset, logverwijdering, herinstallatie of publiek statement zonder incidentleider, tenzij nodig om direct lichamelijk gevaar te stoppen.

61. Triage en ernstniveaus I0 tot en met I4

Incidenten worden geclassificeerd op impact, schaal, gevoeligheid, betrokkenen, operationele verstoring, externe zichtbaarheid en meldplicht.

Kernregels

- I0: observatie of bijna-incident zonder aantoonbare impact.
- I1: beperkt, intern beheersbaar, lage impact.
- I2: significant, meerdere betrokkenen/systemen of gevoelig dossier.
- I3: ernstig, hoog risico, grote operationele verstoring of waarschijnlijk meldplichtig.
- I4: crisis, levens-/waardigheidsrisico, ransomware, massale blootstelling, custody-/identiteitsincident of langdurige uitval.

Werkinstructie

1. Beoordeel vertrouwelijkheid, integriteit en beschikbaarheid.
2. Bepaal aard en hoeveelheid persoonsgegevens en kwetsbaarheid betrokkenen.
3. Beoordeel actieve dreiging, verspreiding en herstelbaarheid.
4. Bepaal contractuele, AVG-, Cbw-, verzekerings- en autoriteitsmeldingen.
5. Herclassificeer zodra feiten veranderen.

Verplichte vastlegging

Ernstscore, argumenten, classificatietijd, beslisser, meldmatrix en herbeoordelingen.

Direct escaleren of stoppen

I3 en I4 worden direct aan directie, privacy en technische leiding gemeld; 24/7 bereikbaarheid is vereist.

Incidentmatrix

Niveau	Indicatie	Minimale actie	Bevoegde leiding
I0	Bijna-incident / geen aantoonbare impact	Registreren, analyseren, lokaal verbeteren	Proceshouder
I1	Beperkt incident, klein bereik, geen gevoelige data	Containment, controle, afsluiten binnen reguliere lijn	Teamleider + security/privacy op afroep
I2	Meerdere betrokkenen, gevoelige gegevens, systeemverstoring	Incidentteam, juridische beoordeling, actieve opvolging	Incidentleider + privacy + IT
I3	Waarschijnlijk hoog risico of meldplicht, grote verstoring	Crisisteam, bestuur, verzekeraar/klant, AP-beoordeling	Directie en incidentleider

Niveau	Indicatie	Minimale actie	Bevoegde leiding
I4	Crisis, ransomware, massale blootstelling, EMS-identiteit/custody	Crisisorganisatie, autoriteiten, continuïteitsplan	Directie/crisisleider 24/7

62. Containment, bewijs en forensische zorgvuldigheid

Incidentrespons beperkt schade zonder relevante informatie te veranderen of vernietigen. Bewijs wordt herleidbaar veiliggesteld.

Kernregels

- Logs, apparaten, e-mails, headers, screenshots, tokens en netwerkgegevens krijgen bron en tijd.
- Toegang tot bewijs is beperkt en gelogd.
- Kopieën worden waar passend hash-gecontroleerd.
- Persoonsgegevens in bewijs worden niet breder gedeeld dan nodig.
- Externe forensische hulp werkt onder contract, geheimhouding en duidelijke instructie.

Werkinstructie

1. Isoleer account, apparaat, koppeling of deel-link proportioneel.
2. Noteer vóór elke wijziging tijd, uitvoerder en reden.
3. Maak veilige kopie van vluchtige gegevens en logs.
4. Bewaar originele bron en werk op kopie waar mogelijk.
5. Registreer chain of custody en overdracht.

Verplichte vastlegging

Bewijsregister, chain of custody, hashes indien gebruikt, wijzigingslog, technische acties en toegang.

Direct escaleren of stoppen

Geen verdachte e-mail doorsturen naar brede groep, geen screenshots met onnodige persoonsgegevens in chat en geen logbestanden overschrijven.

63. Datalekbeoordeling en 72-uursklok

Elk beveiligingsincident met persoonsgegevens wordt beoordeeld als mogelijke inbreuk. Wanneer het waarschijnlijk een risico oplevert voor rechten en vrijheden, meldt DriveBack het datalek in beginsel binnen 72 uur na kennisname aan de AP.

Kernregels

- De klok start bij voldoende zekerheid dat een beveiligingsincident met persoonsgegevens heeft plaatsgevonden, niet pas na volledig onderzoek.
- Niet-melden wordt gemotiveerd en geregistreerd.
- Onvolledige informatie kan gefaseerd worden aangevuld.
- Verwerkers melden zonder onredelijke vertraging aan DriveBack zodat beoordeling mogelijk is.
- Alle datalekken, ook niet-gemelde, komen in het interne datalekregister.

Werkinstructie

1. Bepaal welke persoonsgegevens en betrokkenen zijn geraakt.
2. Beoordeel aard, gevoeligheid, volume, identificatiegemak, gevolgen en maatregelen.
3. Bepaal risico en hoog risico met privacy/juridische functionaris.
4. Laat bevoegde functionaris uiterlijk binnen de interne deadline besluiten over AP-melding.
5. Meld binnen 72 uur of motiveer vertraging; update bij nieuwe feiten.

Verplichte vastlegging

Datalekbeoordeling, kennisnametijd, risicomatrix, besluit, AP-melding/nummer, aanvullingen en niet-meldmotivering.

Juridisch aandachtspunt

De wettelijke 72 uur is een uiterste termijn, geen onderzoekstijd die volledig mag worden verbruikt.

Direct escaleren of stoppen

Direct naar directie/privacy wanneer minder dan 24 uur resteert, feiten onvolledig zijn of betrokkenen mogelijk direct gevaar lopen.

64. Informeren van betrokkenen

Bij waarschijnlijk hoog risico worden betrokkenen onverwijld en in duidelijke taal geïnformeerd, tenzij een wettelijke uitzondering geldt.

Kernregels

- Communicatie beschrijft aard, waarschijnlijke gevolgen, maatregelen en concrete zelfbescherming.
- Geen juridisch jargon, speculatie of onnodige gevoelige details.
- Kanaal is betrouwbaar en bereikt de juiste persoon.
- Bij EMS wordt rekening gehouden met rouw, waardigheid en kwetsbaarheid.
- Publieke communicatie vervangt individuele melding alleen onder toepasselijke voorwaarden.

Werkinstructie

1. Bepaal wie is geraakt en welke contactgegevens betrouwbaar zijn.
2. Stel feitelijke boodschap op en laat privacy/juridisch en communicatie reviewen.
3. Geef contactpunt, handelingsadvies en eventueel fraudewaarschuwing.
4. Verstuur en registreer aflevering/mislukking.
5. Beantwoord vragen, monitor schade en update bij relevante feiten.

Verplichte vastlegging

Betrokkenenlijst, communicatietekst, goedkeuring, verzendbewijs, reacties en nazorg.

Direct escaleren of stoppen

Geen massamail met zichtbare adressen, geen generieke boodschap aan nabestaanden zonder menselijke review en geen vertraging om reputatieredenen.

65. Verkeerde ontvanger, verloren apparaat en onbedoelde publicatie

Veel incidenten ontstaan door verkeerd e-mailadres, deel-link, bijlage, toestelverlies of onbedoelde webpublicatie. De eerste actie is terughalen, blokkeren en verspreiding vaststellen.

Kernregels

- Verzoek tot verwijderen is nuttig maar geen bewijs dat toegang niet heeft plaatsgevonden.
- Deel-links en sessies worden onmiddellijk ingetrokken.
- Vermiste apparaten worden gelokaliseerd, geblokkeerd of gewist via MDM.
- Zoekmachinecache, synchronisaties en downloads worden onderzocht.
- Risico wordt bepaald op inhoud, ontvanger, toegang, beveiliging en verspreiding.

Werkinstructie

1. Meld incident en noteer exact wat is verstuurd/gepubliceerd.
2. Trek link, account, sessie of apparaat in.
3. Neem via betrouwbaar kanaal contact op met ontvanger/platform zonder extra gegevens te delen.

4. Beveilig bewijs van toegang, download en verwijdering.
5. Voer datalekbeoordeling en herstelmaatregelen uit.

Verplichte vastlegging

Verzend-/toegangslog, intrekking, ontvangercontact, verwijderbevestiging, MDM-acties en risicobesluit.

Direct escaleren of stoppen

Geen zelfstandig contact met onbevoegde ontvanger als dit dreiging, afpersing of bewijsverlies kan vergroten; incidentleider beslist.

66. Accountcompromis, phishing en ransomware

Bij vermoeden van accountmisbruik of ransomware wordt de dreiging geïsoleerd, toegang hersteld en laterale verspreiding onderzocht voordat normale werkzaamheden hervatten.

Kernregels

- Wachtwoordwijziging alleen is vaak onvoldoende; tokens, sessies, MFA, mailboxregels en gekoppelde apps worden gecontroleerd.
- Ransomwarebetaling wordt nooit door individuele medewerker besloten.
- Back-ups worden beschermd vóór herstel.
- Autoriteiten, verzekeraar, forensisch specialist en klanten worden volgens meldmatrix betrokken.
- Herstel gebeurt naar schone, geteste omgeving.

Werkinstructie

1. Isoleer getroffen account/apparaat en blokkeer verdachte sessies.
2. Beveilig logs, e-mailheaders, ransom note en systeembeeld.
3. Bepaal bereik, exfiltratie, encryptie en operationele impact.
4. Activeer continuïteitsplan en meldbeoordelingen.
5. Herstel, roteer geheimen, monitor en voer grondoorzaakanalyse uit.

Verplichte vastlegging

Technische tijdlijn, accounts/tokens, indicatoren, exfiltratieanalyse, meldingen, hersteltest en CAPA.

Direct escaleren of stoppen

I4 bij ransomware in dossier-, meldkamer-, EMS-, back-up- of identityomgeving, of aanwijzing dat gegevens zijn buitgemaakt.

67. Leveranciersincidenten en ketenrespons

Een incident bij AFAS, cloud, telefonie, GPS, hotel-/reispartner of buitenlandse ketenpartner kan DriveBack direct raken. Contractuele melding en eigen beoordeling blijven noodzakelijk.

Kernregels

- DriveBack wacht niet passief op een eindrapport wanneer eigen betrokkenen risico lopen.
- Leverancier verstrekt feiten, tijdlijn, data, systemen, maatregelen en subverwerkers.
- DriveBack bepaalt zelf AVG- en contractuele meldingen als verantwoordelijke.
- Toegang of koppeling kan tijdelijk worden opgeschort.
- Herstart vereist herstel- en vertrouwenstoets.

Werkinstructie

1. Open eigen incident en bevestig kennisnametijd.
2. Vraag gestandaardiseerde incidentinformatie en bewijs.

3. Bepaal eigen data, betrokkenen, continuïteit en meldplichten.
4. Beperk koppelingen of accounts indien nodig.
5. Evalueer contract, herstel, CAPA en voortzetting.

Verplichte vastlegging

Leveranciersmelding, vragenlijst, eigen beoordeling, koppelingacties, communicatie en evaluatie.

Direct escaleren of stoppen

Escaleren bij vertraging, onvolledige informatie, onbekende subverwerker, buitenlandse exfiltratie of herhaald incident.

68. EMS-kritieke privacy- en custody-incidenten

Misidentificatie, verkeerde documenten, sealbreuk, verloren custody, onbevoegde overdracht of ongepaste beeldregistratie vereisen onmiddellijke operationele stop en gecombineerde privacy-, waardigheids- en juridische respons.

Kernregels

- De fysieke en administratieve keten worden tegelijk veiliggesteld.
- Geen correctie door oorspronkelijke gegevens stilzwijgend te overschrijven.
- Nabestaandencommunicatie gebeurt door aangewezen senior functionaris.
- Autoriteiten, verzekeraar en ketenpartners worden afgestemd op feitelijke rol.
- Beelden en documenten worden zeer beperkt gedeeld.

Werkinstructie

1. Zet overdracht/transport op HOLD en waarborg waardige veilige situatie.
2. Controleer identiteit, vrijgave, seal, documenten en custody met twee bevoegde personen.
3. Open I4-incident en beveilig alle fysieke/digitale bewijsstukken.
4. Bepaal noodzakelijke autoriteits-, klant-, AP- en betrokkenenmelding.
5. Herstart alleen na schriftelijke vrijgave en herstelplan.

Verplichte vastlegging

EMS-incidentdossier, custodyketen, seal-/documentcontrole, beslissingen, communicatie, herstartvrijgave en nazorg.

Direct escaleren of stoppen

Geen verdere overdracht, openen, fotograferen of aanpassen zonder bevoegde incidentleiding en toepasselijke autoriteit.

69. Externe meldmatrix: AP, Cbw, politie, verzekeraar en opdrachtgever

Eén incident kan meerdere meld- en informatieplichten activeren. DriveBack gebruikt een meldmatrix met eigenaar, trigger, termijn, kanaal en minimale inhoud.

Kernregels

- AVG-melding aan de AP staat los van contractuele klantmelding.
- Cbw-melding geldt alleen indien DriveBack of de betreffende activiteit onder de wet valt en het incident significant is.
- Politiecontact is passend bij fraude, diefstal, afpersing, bedreiging of ander strafbaar feit.
- Verzekeraar wordt tijdig volgens polisvoorwaarden geïnformeerd zonder onnodige erkenning van aansprakelijkheid.
- Opdrachtgever ontvangt feitelijke informatie volgens rol en contract.

Werkinstructie

1. Identificeer alle toepasselijke regimes en contracten.

2. Bepaal trigger, kennisnametijd, termijn en beslissingsbevoegde.
3. Stem inhoud af zodat meldingen consistent maar doelgericht zijn.
4. Registreer ontvangst, zaaknummer en vervolgvragen.
5. Werk meldingen bij en sluit pas na definitieve rapportage.

Verplichte vastlegging

Meldmatrix, besluiten, verzonden meldingen, ontvangstnummers, updates en eindrapport.

Direct escaleren of stoppen

Geen externe melding uitstellen omdat andere melding nog niet volledig is; gebruik gefaseerde informatie waar toegestaan.

70. Post-incidentreview en corrigerende maatregelen

Na beheersing onderzoekt DriveBack grondoorzaak, effectiviteit van respons en structurele verbeteringen zonder te vervallen in schuldtoewijzing aan één persoon.

Kernregels

- Feitelijke tijdlijn en systeemoorzaken worden gescheiden van aannames.
- Mens, proces, technologie, organisatie en leverancier worden allemaal beoordeeld.
- CAPA heeft eigenaar, prioriteit, deadline en effectiviteitstest.
- Ernstige incidenten worden in managementreview besproken.
- Relevante lessen worden geanonimiseerd in training en procedures verwerkt.

Werkinstructie

1. Plan review kort na stabilisatie en met betrokken disciplines.
2. Analyseer directe oorzaak, achterliggende oorzaken en gemiste detectiekansen.
3. Bepaal herstel, preventie, detectie en responsverbeteringen.
4. Voer maatregelen uit en test aantoonbaar.
5. Sluit incident alleen na bestuurs-/eigenaaracceptatie van restrisico.

Verplichte vastlegging

Post-incidentrapport, root cause, CAPA, testbewijs, beleidswijziging, training en afsluitbesluit.

Direct escaleren of stoppen

Herhaald incident met dezelfde oorzaak of overschreden P0-deadline wordt naar directie geëscaleerd.

DEEL VI

GPS EN MONITORING

Rechtmatig, transparant en proportioneel gebruik van locatie-, telematica-, camera- en gespreksgegevens

71. Doelen en verboden gebruik van GPS

GPS en telematica worden uitsluitend gebruikt voor veiligheid, dispatch, routecoördinatie, check-ins, diefstal-/incidentrespons en aantoonbare uitvoering voor zover noodzakelijk.

Kernregels

- Live locatie is alleen zichtbaar voor operationele rollen tijdens actieve inzet.
- GPS is niet bedoeld voor permanente controle van pauzes, privégedrag of algemene productiviteit.
- Geen geheime tracker of verborgen activering.
- Doeluitbreiding vereist nieuwe LIA/DPIA, transparantie en medezeggenschapsbeoordeling.
- Gebruik voor disciplinaire beoordeling is uitzonderlijk en vereist afzonderlijke juridische toets.

Werkinstructie

1. Beschrijf per voertuig/app het concrete doel en de gebruikersgroep.
2. Bepaal of continue tracking nodig is of mijlpaal/check-in volstaat.
3. Stel trackingvenster, zichtbare status en uitschakelroute in.
4. Informeer medewerkers, chauffeurs en waar relevant klanten.
5. Controleer gebruik en verwijder doelvreemde data.

Verplichte vastlegging

GPS-register, doel, grondslag, LIA/DPIA, gebruikersrollen, trackingvenster en review.

Direct escaleren of stoppen

Tracking blokkeren wanneer doel onduidelijk is, voertuig privé wordt gebruikt of medewerkers niet aantoonbaar zijn geïnformeerd.

72. Grondslag, LIA, DPIA en medezeggenschap voor GPS

GPS-gebruik wordt vooraf beoordeeld op grondslag, noodzakelijkheid, minder ingrijpende alternatieven, belangenafweging en mogelijk hoog risico.

Kernregels

- Gerechtvaardigd belang vereist concrete LIA; contract of toestemming is niet automatisch passend.
- Systematische observatie kan een DPIA verplicht maken.
- Een ondernemingsraad heeft instemmingsrecht bij een regeling voor personeelsvolgsystemen; bij groei wordt ook PVT/medezeggenschap tijdig betrokken.
- De beoordeling omvat werknemers, oproepchauffeurs, ingehuurde krachten en privégebruik.

- Technische standaardmogelijkheden van leverancier zijn geen noodzakelijkheid.

Werkinstructie

1. Voer GPS-screening uit per use case en voertuigcategorie.
2. Beschrijf belang, alternatieven, impact, frequentie, retentie en ontvangers.
3. Voer DPIA uit wanneer waarschijnlijk hoog risico bestaat.
4. Vraag medezeggenschapsinstemming waar wettelijk vereist.
5. Laat directie livegang en restrisico formeel goedkeuren.

Verplichte vastlegging

LIA, DPIA, OR/PVT-besluit, privacyinformatie, configuratie en bestuursbesluit.

Direct escaleren of stoppen
Geen livegang zonder formele beoordeling en vereiste medezeggenschapsroute.

73. Operationele GPS-werkinstructie

Tijdens een actieve opdracht ondersteunt GPS de meldkamer bij veiligheid en planning zonder de chauffeur onnodig te volgen.

Kernregels

- Tracking start bij formele dispatch of vertrek en eindigt bij overdracht/einde dienst.
- De chauffeur ziet of weet dat tracking actief is.
- Meldkamer raadpleegt live locatie alleen voor concrete operationele reden.
- Afwijkingen leiden eerst tot contact en context, niet automatisch tot oordeel.
- Systeemuitval wordt opgevangen met afgesproken check-ins.

Werkinstructie

1. Controleer vóór vertrek apparaat, privacyinformatie en trackingstatus.
2. Koppel tracking aan juiste zaak en chauffeur.
3. Gebruik locatie voor ETA, veiligheid, contactverlies en incident; leg bijzondere raadpleging vast.
4. Stop of ontkoppel na overdracht/einde dienst.
5. Controleer dat ruwe route automatisch in retentiecyclus komt.

Verplichte vastlegging

Zaakkoppeling, trackingstart/-stop, gebruikersraadpleging, afwijkingsnotitie en retentietrigger.

Direct escaleren of stoppen
Direct incidentmelding bij verkeerde zaakkoppeling, tracking na dienst, publiek deelbare link of onbevoegde live-inzage.

74. Privégebruik, rust en uitschakelen

Buiten actieve inzet of bij toegestaan privégebruik wordt locatieverwerking uitgeschakeld of technisch afgescheiden, behalve wanneer een beperkte anti-diefstalfunctie aantoonbaar noodzakelijk en transparant is.

Kernregels

- Rusttijd is geen vrijbrief voor continue prestatiecontrole.
- Privéritten worden niet inhoudelijk gevolgd.
- Uitschakelen mag veiligheid niet ongemerkt aantasten; alternatieve check-in wordt afgesproken.
- Geen negatieve beoordeling omdat een medewerker rechtmatig privacyfunctie gebruikt.

- Anti-diefstaldata is beperkt toegankelijk en wordt alleen bij concrete aanleiding bekeken.

Werkinstructie

1. Definieer dienst-, rust- en privéstatus in systeem.
2. Configureer automatische stop of privacy mode.
3. Instrueer chauffeur hoe status zichtbaar en corrigeerbaar is.
4. Leg uitzonderingen en anti-diefstaltoegang vast.
5. Controleer periodiek op tracking buiten toegestaan venster.

Verplichte vastlegging

Privacy-modeconfiguratie, instructie, uitzonderingslog, anti-diefstalraadpleging en audit.

Direct escaleren of stoppen

Tracking buiten dienst zonder geldige uitzondering wordt als mogelijk datalek en personeelsprivacy-incident beoordeeld.

75. GPS-retentie, toegang en rapportage

Ruwe GPS-routehistorie wordt kort bewaard. Voor aantoonbare uitvoering worden waar mogelijk alleen noodzakelijke mijlpalen, aankomst/vertrek en incidentrelevante fragmenten in het dossier opgenomen.

Kernregels

- Intern uitgangspunt voor ruwe route: 90 dagen, te bekrachtigen en waar mogelijk verkorten.
- Zaakmijlpalen kunnen volgens operationele dossierretermijn worden bewaard.
- Bulkexport en historische zoekfunctie zijn beperkt.
- Klanten ontvangen alleen contractueel noodzakelijke rapportage, geen volledige personeelsroute.
- Incidentfragment wordt geselecteerd en onder legal hold geplaatst; overige data volgt normale retentie.

Werkinstructie

1. Configureer automatische verwijdering van ruwe data.
2. Bepaal per rapport het doel en minimale locatievelden.
3. Laat export goedkeuren en registreer ontvanger.
4. Selecteer incidentfragment met begin/eind en reden.
5. Controleer maandelijks retentie en uitzonderingen.

Verplichte vastlegging

Retentieconfiguratie, exportlog, rapportdefinitie, incidentselectie en verwijdersteekproef.

Direct escaleren of stoppen

Geen onbeperkte route-export aan opdrachtgever of bewaren van volledige geschiedenis vanwege algemene “kwaliteitscontrole”.

76. Telematica, rijgedrag en voertuigdiagnostiek

Snelheid, remmen, acceleratie, foutcodes, brandstof en voertuigdiagnostiek kunnen persoonsgegevens zijn wanneer zij aan een chauffeur zijn te koppelen en worden daarom doelgericht beheerd.

Kernregels

- Veiligheidsanalyse is gescheiden van automatische prestatie- of sanctiescore.
- Ruwe sensordata wordt niet langer bewaard dan nodig.
- Context zoals weer, voertuigtype, route en noodsituatie wordt betrokken.

- Geen volledig geautomatiseerde personeelsbeslissing op telematicascore.
- Leveranciers mogen data niet voor eigen training/marketing hergebruiken zonder geldige basis.

Werkinstructie

1. Definieer welke telematicavelden nodig zijn en voor welk doel.
2. Voer LIA/DPIA en werknemersinformatie uit.
3. Beperk toegang en stel context-/reviewprocedure vast.
4. Onderzoek veiligheidsafwijking met hoor en wederhoor.
5. Verwijder ruwe data en monitor leveranciersgebruik.

Verplichte vastlegging

Telematicaregister, veldlijst, beoordeling, rapport, hoor/wederhoor, retentie en leverancierstoezicht.

Direct escaleren of stoppen

Geen disciplinaire maatregel uitsluitend op een onverklaarde algoritmische score of enkel GPS-datapunt.

77. Dashcams, voertuigcamera's en gebouwcamera's

Camera's worden alleen ingezet bij aantoonbare noodzaak, afgebakend beeldgebied, duidelijke informatie, korte retentie en beperkte toegang.

Kernregels

- Geen camera gericht op rustruimte, kleedruimte, sanitaire ruimte of structureel op bestuurdersgezicht zonder uitzonderlijke rechtvaardiging.
- Audio staat standaard uit.
- Dashcam slaat bij voorkeur gebeurtenisgericht en lokaal versleuteld op.
- Beelden worden niet voor sociale media of training gebruikt zonder aparte basis.
- Interne standaardretentie is maximaal 28 dagen tenzij incident/legal hold.

Werkinstructie

1. Beschrijf doel, gebied, tijden, functies en alternatieven.
2. Voer LIA/DPIA en medezeggenschapsroute uit.
3. Plaats informatie en configureer maskering, toegang en retentie.
4. Beveilig export en registreer iedere inzage.
5. Review noodzaak en effectiviteit minimaal jaarlijks.

Verplichte vastlegging

Cameraplan, DPIA/LIA, plattegrond/zichtveld, informatiebord, toegang, export en verwijdering.

Direct escaleren of stoppen

Heimelijke camera-inzet of structurele observatie van personeel vereist vooraf specialistisch juridisch advies en mag niet als gewone maatregel worden toegepast.

78. Gespreksopnamen, meeluisteren en transcriptie

Telefoongesprekken worden alleen opgenomen of live gemonitord voor vooraf vastgestelde doelen zoals bewijs, veiligheid of kwaliteitsverbetering en met passende informatie.

Kernregels

- Opname staat niet standaard aan zonder formeel besluit.
- Medewerkers en externe gesprekspartners worden duidelijk geïnformeerd.
- Kwaliteitsbeoordeling gebruikt beperkte steekproef en objectieve criteria.

- Opnamen worden niet breed beschikbaar gemaakt en intern uitgangspunt is 90 dagen.
- AI-transcriptie vereist aparte leveranciers- en gegevensbeoordeling.

Werkinstructie

1. Bepaal doel, grondslag, noodzakelijkheid en alternatieven.
2. Voer LIA/DPIA en medezeggenschapsbeoordeling uit.
3. Configureer mededeling, toegang, export en automatische verwijdering.
4. Selecteer en registreer kwaliteits-/incidentgebruik.
5. Verwijder na termijn en audit steekproefsgewijs.

Verplichte vastlegging

Opnamebeleid, LIA/DPIA, informatietekst, toegangslog, beoordeling, export en verwijdertest.

Direct escaleren of stoppen

Geen heimelijk meeluisteren, onbeperkt terugluisteren of gebruik voor ander doel zonder nieuwe beoordeling.

79. Audit, klachten en opschorting van monitoring

Monitoringmiddelen worden periodiek getoetst op werkelijke noodzaak, effectiviteit, foutmarges, medewerkersimpact en doelverschuiving.

Kernregels

- Klachten en bezwaren worden onafhankelijk onderzocht.
- Onjuiste tracking of foutieve koppeling wordt gecorrigeerd en als incident beoordeeld.
- Een systeem kan tijdelijk worden uitgeschakeld wanneer rechten of retentie niet werken.
- Leverancierswijzigingen worden vooraf beoordeeld.
- Bevindingen gaan naar managementreview en medezeggenschap waar passend.

Werkinstructie

1. Audit configuratie, gebruikers, raadplegingen, retentie en privacy mode.
2. Vergelijk feitelijk gebruik met LIA/DPIA en privacyinformatie.
3. Onderzoek klachten en afwijkingen met logs.
4. Schort onrechtmatig of onbeheerst gebruik op.
5. Implementeer CAPA en herstart alleen na verificatie.

Verplichte vastlegging

Monitoringaudit, klacht, incident, opschortingsbesluit, CAPA en herstartvrijgave.

Direct escaleren of stoppen

Onmiddellijke HOLD bij verborgen doeluitbreiding, tracking buiten dienst, ontbrekende automatische verwijdering of brede onbevoegde toegang.

DEEL VII

DRIVEBACK MOBILITEITSCONTINUÏTEIT

Bijzondere privacy- en beveiligingsregels voor personen, voertuigen, reizen en vervangende chauffeurs

80. Mobiliteitsintake: melder, bestuurder en passagiers

Bij een mobiliteitsmelding verzamelt DriveBack alleen informatie die nodig is om bevoegdheid, veiligheid, voertuig, locatie, reis en terugkeer te organiseren.

Kernregels

- De melder kan verschillen van bestuurder, eigenaar, verzekerde of opdrachtgever; rollen worden vastgelegd.
- Contactgegevens van passagiers worden alleen opgenomen wanneer noodzakelijk.
- Minderjarigen en kwetsbare personen krijgen verhoogde bescherming.
- Relatieconflicten, scheiding of familieomstandigheden worden niet onnodig gedocumenteerd.
- Noodcontacten worden alleen voor het afgesproken doel gebruikt.

Werkinstructie

1. Identificeer melder, opdrachtgever, bestuurder, eigenaar en noodzakelijke contactpersonen.
2. Leg bevoegdheid en voorkeurskanaal vast.
3. Vraag alleen operationele beperkingen, locatie, voertuig en reisbehoefte.
4. Markeer kwetsbaarheid zonder overbodige details.
5. Bevestig privacyinformatie en corrigeer gegevens vóór dispatch.

Verplichte vastlegging

Mobiliteitsintake, rolverdeling, bevoegdheidsbewijs, contactvoorkeur, privacy-informatie en correcties.

Direct escaleren of stoppen

Geen volledige familie- of medische geschiedenis opnemen om een vervangende chauffeur te plannen.

81. Ziekte, uitval en functionele medische informatie

Bij ziekte of uitval registreert DriveBack uitsluitend wat nodig is om aantoonbare uitval, veilige inzet en passende terugkeer te beoordelen.

Kernregels

- Vraag niet standaard naar diagnose, behandeling, medicatie of medisch dossier.
- Registreer functioneel: bestuurder kan niet verantwoord rijden, verwachte duur indien bekend, mobiliteitsbeperking en benodigde begeleiding.
- Medisch bewijs wordt alleen gevraagd wanneer contract/abonnement dit rechtmatig en proportioneel vereist.
- Bewijs wordt sterk afgeschermd en kort bewaard.
- Bij medische noodsituatie gaat veiligheid vóór administratie.

Werkinstructie

1. Bepaal welke functionele informatie voor uitvoering nodig is.
2. Leg bewijsstatus vast zonder volledige inhoud te kopiëren waar mogelijk.
3. Beperk toegang tot aangewezen intake/claimrol.
4. Deel met chauffeur alleen praktische veiligheidsinformatie.
5. Verwijder bewijs na doelbereik volgens matrix.

Verplichte vastlegging

Functionele uitvalregistratie, bewijsnoodzaak, toegangslog, minimale chauffeursinstructie en verwijdering.

Direct escaleren of stoppen

Geen medische diagnose in chauffeursbriefing, factuuromschrijving of algemene klantnotitie.

82. Voertuig-, kenteken-, sleutel- en verzekeringsgegevens

Voertuiggegevens worden verwerkt voor identificatie, bevoegdheid, verzekering, technische veiligheid, route en overdracht.

Kernregels

- Kenteken en chassisnummer kunnen persoonsgegevens zijn wanneer aan een natuurlijke persoon gekoppeld.
- Sleutelcodes en voertuiglocatie zijn ZEER VERTROUWELIJK vanwege diefstalrisico.
- Verzekeringsinformatie wordt alleen gedeeld met bevoegde partijen.
- Voertuigprofielen worden niet zonder basis voor marketing hergebruikt.
- Historische voertuigdata wordt niet automatisch aan nieuwe eigenaar/opdracht gekoppeld.

Werkinstructie

1. Verifieer voertuig en bevoegdheid via documenten of betrouwbare partner.
2. Registreer minimale technische en verzekeringskenmerken.
3. Beheer sleutel- en documentcustody met overdracht.
4. Deel locatie en toegangscode alleen vlak vóór noodzakelijke inzet.
5. Sluit toegang en verwijder tijdelijke codes na overdracht.

Verplichte vastlegging

Voertuigdossier, verificatie, sleutelcustody, deelhistorie, code-intrekking en overdrachtsbewijs.

Direct escaleren of stoppen

Direct incidentmelding bij verloren sleutel, gelekte voertuiglocatie, verkeerde kentekenkoppeling of onbevoegde toegangscode.

83. Reis, hotel, ticketing en buitenlandse partners

Reis- en verblijfsgegevens worden gedeeld op need-to-knowbasis met vervoerders, hotels, taxi's en partners en niet als volledig operationeel dossier.

Kernregels

- Paspoortgegevens worden alleen verstrekt wanneer de vervoerder of autoriteit dit vereist.
- Hotel ontvangt geen medische of EMS-achtergrond als alleen kamer en aankomsttijd nodig zijn.
- Persoonlijke reisaccounts en loyaliteitsprofielen worden niet zonder toestemming gebruikt.
- Buitenlandse partnercontacten worden geverifieerd.
- Reisschema's van medewerkers en klanten zijn vertrouwelijk vanwege veiligheidsrisico.

Werkinstructie

1. Bepaal per leverancier minimale reserveringsgegevens.
2. Gebruik zakelijke boekingsaccounts en goedgekeurde betaalroute.
3. Verifieer ontvanger en land/doorgifte.
4. Leg boekingsreferentie in zaak vast zonder onnodige kopieën.
5. Verwijder tijdelijke tickets/ID-kopieën van apparaat na inzet.

Verplichte vastlegging

Boekingslog, ontvangers, doorgiftebeoordeling, reisreferentie, kostenbewijs en verwijdering.

Direct escaleren of stoppen

Geen volledige zaakomschrijving of gezondheidsdetails in vrij tekstveld van hotel- of taxi-reservering.

84. Verzekeraars, fleetklanten, alarmcentrales en opdrachtgeversportalen

B2B-opdrachtgevers ontvangen alleen informatie die nodig is voor opdracht, dekking, voortgang, kosten en bewijs, in overeenstemming met de vastgestelde AVG-rol.

Kernregels

- Een klantportaal krijgt individuele accounts, MFA, roltoegang en logging.
- Opdrachtgever mag niet standaard volledige gezondheids-, GPS- of communicatiegegevens ontvangen.
- Rapporten maken onderscheid tussen feit, bron, beoordeling en persoonlijk detail.
- Contractuele rapportage-eisen worden vooraf privacygetoetst.
- Bulkdownload of toegang tot meerdere klanten/verzekerden is beperkt.

Werkinstructie

1. Bepaal privacyrol en contractuele dataset.
2. Maak gestandaardiseerd minimaal rapport.
3. Configureer klantaccount en zaakafscherming.
4. Controleer export/portaaltoegang en verwijder verlopen accounts.
5. Audit steekproefsgewijs wat klanten werkelijk kunnen zien.

Verplichte vastlegging

Rolbeoordeling, rapportdefinitie, portaalaccount, toegangslog, export en audit.

Direct escaleren of stoppen

Geen automatische doorgifte van volledige GPS-route, medische bijlage of interne incidentnotitie zonder expliciete noodzaak.

85. Voertuiginspectie, foto’s en overdrachtsrapportage

Inspectiegegevens bewijzen conditie en veilige overdracht, maar worden zo vastgelegd dat personen, woningen, bagage en documenten niet onnodig herkenbaar zijn.

Kernregels

- Foto’s volgen vaste schadelijst en overzichtshoeken.
- Kenteken mag zichtbaar zijn wanneer nodig voor identificatie; privé-documenten worden afgeschermd.
- Interieurfoto’s beperken zich tot noodzakelijke conditie.
- Persoonlijke bezittingen worden geïnventariseerd zonder onnodig intieme details.
- Ontvanger tekent of bevestigt digitaal via geverifieerd kanaal.

Werkinstructie

1. Controleer omgeving en verwijder/bedek gevoelige stukken waar mogelijk.
2. Maak alleen vereiste foto’s met zakelijk apparaat.
3. Upload en koppel direct; verwijder lokale kopie.
4. Maak feitelijk overdrachtsrapport en laat ontvanger verifiëren.
5. Start claim/legal hold alleen voor relevante set.

Verplichte vastlegging

Foto-index, conditierapport, uploadcontrole, overdrachtsbewijs, claimselectie en retentie.

Direct escaleren of stoppen

Geen foto’s delen in openbare groepschat of gebruiken voor promotie zonder aparte rechtmatige toestemming en rechtencontrole.

DEEL VIII

DRIVEBACK EUROPEAN MORTUARY SERVICES

Streng afgeschermde gegevensverwerking bij Europees A-naar-B-overledenenvervoer

86. EMS-scope en gegevensdiscipline

DriveBack EMS beperkt zich tot het organiseren en uitvoeren van waardig Europees vervoer van een reeds overleden persoon in gesloten kist of andere toegestane gesloten voorziening van A naar B. Het dossier volgt die afgebakende taak.

Kernregels

- EMS organiseert niet zelfstandig de uitvaart, balseming, postmortale verzorging, formele identificatie, langdurige bewaring of afscheid.
- Gegevens buiten de transporttaak worden niet verzameld “voor volledigheid”.
- Opdrachtgever, vrijgevende partij en ontvangende professional houden hun eigen wettelijke verantwoordelijkheden.
- Iedere uitbreiding van de scope vereist vooraf juridische, operationele en privacybeoordeling.
- De EMS-zaak is standaard ZEER VERTROUWELIJK.

Werkinstructie

1. Leg de transportopdracht, herkomst, bestemming, opdrachtgever en professionele ketenrollen vast.
2. Controleer dat de opdracht binnen de vastgestelde EMS-scope valt.
3. Vraag uitsluitend documenten en veiligheidsinformatie voor vervoer en overdracht.
4. Wijs afwijkende verzoeken af of verwijs naar bevoegde professional.
5. Registreer scopebesluit en eventuele escalatie.

Verplichte vastlegging

EMS-opdracht, scopecheck, rollen, documentlijst, afwijkingsbesluit en overdracht.

Direct escaleren of stoppen

NO-GO bij verzoek om formele identificatie, openen van de kist, postmortale verzorging of andere activiteit waarvoor DriveBack niet bevoegd of ingericht is.

87. Overledene, nabestaanden en levende betrokkenen

Hoewel gegevens die uitsluitend de overledene betreffen niet rechtstreeks door de AVG worden beschermd, bevat een EMS-dossier vaak gegevens van nabestaanden, melders, professionals en medewerkers die wel persoonsgegevens zijn.

Kernregels

- Nabestaandencontact wordt met bijzondere zorg, minimale registratie en beperkte toegang verwerkt.
- Familieverhoudingen en emoties worden alleen vastgelegd wanneer operationeel noodzakelijk.
- De waardigheid van de overledene geldt als zelfstandige interne norm.
- Informatie over doodsoorzaak of omstandigheden wordt niet breder gedeeld dan nodig.
- Privacyrechten worden beoordeeld op wiens gegevens het verzoek betrekking heeft.

Werkinstructie

1. Scheid contact-/contractgegevens van de professionele transportdocumentset.
2. Markeer levende betrokkenen en hun rollen.
3. Beperk vrije tekst over familie en omstandigheden.
4. Verstrek informatie en contactpunt aan opdrachtgever/nabestaande.
5. Controleer ontvangers en toegang bij ieder dossierdeel.

Verplichte vastlegging

Betrokkenenoverzicht, privacyinformatie, toegangslog, ontvangers en verzoekenregistratie.

Direct escaleren of stoppen

Geen details over doodsoorzaak, locatie of familie delen met chauffeur, partner of opdrachtgever wanneer alleen vervoerstatus nodig is.

88. Identificatiegegevens, vrijgave en documentcontrole

DriveBack verifieert dat bevoegde partijen de overledene en transportdocumenten correct hebben gekoppeld; DriveBack neemt niet de formele identificatietaak van autoriteiten of professionals over.

Kernregels

- Naam, geboortedatum, overlijdensdatum, documentnummer en kist-/sealreferentie worden via vierogencontrole gekoppeld.
- Onzekerheid of tegenstrijdigheid wordt niet “praktisch opgelost” door raden.
- Bron en status van documenten zijn herleidbaar.
- Kopieën worden geminimaliseerd en zeer beperkt toegankelijk.
- Correcties gebruiken addendum en laten oorspronkelijke informatie zichtbaar.

Werkinstructie

1. Ontvang documenten via beveiligd kanaal van geverifieerde partij.
2. Vergelijk kernidentificatoren met vrijgave, kistlabel en opdracht.
3. Laat tweede bevoegde medewerker controleren.
4. Markeer compleet, ontbrekend, ongeldig of conflicterend.
5. Dispatch pas na formele documentvrijgave.

Verplichte vastlegging

Documentcheck, vierogencontrole, bron, vrijgavestatus, afwijkingen en dispatchbesluit.

Direct escaleren of stoppen

Onmiddellijke HOLD bij verschil in naam, datum, documentnummer, kistlabel, seal of ontvangende partij.

89. Custody, seal en overdrachtsregistratie

De fysieke en digitale custodyketen bewijst wie wanneer verantwoordelijk was voor de gesloten kist, documenten, seal en eventuele persoonlijke bezittingen.

Kernregels

- Iedere overdracht bevat datum/tijd, locatie, overdrager, ontvanger, bevoegdheid en conditie.
- Sealnummer en zichtbare integriteit worden gecontroleerd zonder ongeoorloofd openen.
- Digitale custodywijziging volgt de fysieke overdracht onmiddellijk.
- Geen overdracht aan een persoon die niet vooraf of via bevoegde route is geverifieerd.
- Custodybewijs is niet aanpasbaar zonder audittrail.

Werkinstructie

1. Verifieer overdragende partij, documenten, kist, seal en voertuigconditie.
2. Registreer ontvangst met twee EMS-crewleden.
3. Beveilig documenten en toegang gedurende vervoer.
4. Verifieer ontvanger via bekende professionele contactroute.
5. Laat overdracht tekenen/bevestigen en sluit custodyketen.

Verplichte vastlegging

Custodycertificaat, sealnummer, identiteit/bevoegdheid partijen, tijdlijn, afwijkingen en ontvangstbewijs.

Direct escaleren of stoppen

I4 en transport-HOLD bij sealbreuk, verdwenen documenten, onbevoegde ontvanger, custodygat of vermoeden van verwisseling.

90. Gezondheids-, infectie- en blootstellingsinformatie

EMS verwerkt uitsluitend de functionele risico-informatie die nodig is voor veilige PBM-keuze, vervoer, reiniging en eventuele incidentrespons.

Kernregels

- Volledige medische historie of diagnose is niet nodig voor standaardtransport.
- Infectie-/blootstellingsinformatie krijgt toegang voor aangewezen EMS- en veiligheidsrollen.
- Crew ontvangt praktische maatregelen, niet meer medische details dan noodzakelijk.
- Blootstellingsincidenten worden apart beveiligd als personeelsgezondheidsinformatie.
- Delen met partner of ontvanger volgt professionele noodzaak en wettelijke kaders.

Werkinstructie

1. Vraag aan vrijgevende professional naar relevante functionele voorzorgsmaatregelen.
2. Registreer risicocategorie en vereiste PBM/handeling.
3. Brief crew in minimale duidelijke taal.
4. Voer reiniging/desinfectie en registraties uit.
5. Bij blootstelling: stop, volg veiligheidsprotocol en scheid medisch dossier.

Verplichte vastlegging

EMS-risicoinstructie, PBM-plan, crewbriefing, reinigingslog, blootstellingsincident en beperkte toegang.

Direct escaleren of stoppen

Geen doodsoorzaak of medische details in algemene ritplanning, hotelboeking, factuur of gedeelde groepschat.

91. Fotografie, beeld, waardigheid en mediaverbod

Fotografie van de overledene is niet toegestaan als standaard identificatie- of bewijsinstrument. Beeldregistratie beperkt zich tot voertuig, gesloten kist, labels/seal of schade voor zover noodzakelijk en waardig.

Kernregels

- Geen herkenbaar beeld van de overledene zonder uitzonderlijke wettelijke/professionele noodzaak en formele toestemming.
- Geen selfie, promotiebeeld, socialmediapost of informele crewfoto tijdens EMS-opdracht.
- Omstanders, nabestaanden en privéomgevingen worden vermeden.
- Beeldapparaat is zakelijk beheerd en upload gebeurt direct.
- Toegang en retentie zijn streng beperkt.

Werkinstructie

1. Bepaal vooraf welke zakelijke bewijsbeelden nodig zijn.
2. Controleer waardigheid, achtergrond en gevoelige informatie.
3. Maak beeld alleen met goedgekeurd apparaat.
4. Upload direct naar EMS-zaak en verwijder lokaal.
5. Laat afwijkend beeldgebruik door directie/privacy/juridisch beoordelen.

Verplichte vastlegging

Beeldindex, doel, maker, upload, toegang, afwijkingsbesluit en verwijdering.

Direct escaleren of stoppen

Direct I3/I4-incident bij ongepaste foto, privé-opslag, externe verspreiding of herkenbaar beeld van de overledene.

92. Persoonlijke bezittingen, paspoort en waardestukken

Persoonlijke bezittingen en identiteitsdocumenten worden alleen meegenomen wanneer opdracht, bevoegdheid en ontvangende partij dit duidelijk toestaan; ieder item volgt een aparte custodyregistratie.

Kernregels

- Waarde, hoeveelheid en conditie worden feitelijk beschreven zonder onnodige inhoudelijke inspectie.
- Gesloten tassen of verzegelde pakketten worden niet zonder bevoegdheid geopend.
- Paspoort en officiële documenten worden apart beveiligd.
- Waardevolle of gevoelige items kunnen worden geweigerd of via gespecialiseerde route gaan.
- Ontvangst wordt afzonderlijk bevestigd.

Werkinstructie

1. Controleer opdrachtbevoegdheid en inventarislijst.
2. Verpak, label en registreer itemnummer/seal.
3. Beperk toegang en houd fysiek gescheiden van algemene bagage.
4. Verifieer ontvanger en laat ontvangst per item bevestigen.
5. Registreer afwijking, schade of ontbrekend item direct.

Verplichte vastlegging

Inventaris, custody, seal, conditie, weigering/afwijking en ontvangstbewijs.

Direct escaleren of stoppen

I3-incident bij vermissing, onbevoegd openen, onbekend waarde-item of identiteitsdocument zonder duidelijke ontvanger.

93. Buitenlandse autoriteiten, partners en internationale gegevensdeling

EMS-opdrachten vereisen vaak uitwisseling met uitvaartondernemers, mortuaria, consulaten, politie, gemeenten, ferry- of luchthavenpartijen. Iedere ontvanger wordt geverifieerd en ontvangt de minimale noodzakelijke set.

Kernregels

- Professionele titel of logo alleen bewijst geen bevoegdheid.
- Land-, transit- en bestemmingsvereisten worden uit officieel of gevalideerd landenregister gecontroleerd.
- Doorgifte buiten de EER krijgt juridische beoordeling waar persoonsgegevens van levende betrokkenen worden gedeeld.
- Vertalingen worden gecontroleerd en als versie beheerd.
- E-mailadressen en bank-/documentverzoeken worden via tweede kanaal geverifieerd.

Werkinstructie

1. Identificeer land, autoriteit/partner, rol en bevoegd contact.
2. Bepaal documenten en persoonsgegevens die noodzakelijk zijn.
3. Controleer doorgiftebasis, beveiligd kanaal en taal/vertaling.
4. Registreer verzending, ontvangst en eventuele vragen.
5. Beëindig tijdelijke toegang en archiveer alleen kernbewijs.

Verplichte vastlegging

Partnerverificatie, landencheck, doorgiftebeoordeling, verzendlog, vertaling en ontvangst.

Direct escaleren of stoppen

Geen volledige EMS-zaak naar generiek buitenlands e-mailadres of onbevestigde tussenpersoon sturen.

94. EMS-retentie, beperkte toegang en waardige afsluiting

Na professionele overdracht wordt de EMS-zaak gecontroleerd, tijdelijke toegang ingetrokken en ruwe of overbodige informatie verwijderd, terwijl kernbewijs volgens bekrachtigde termijn blijft.

Kernregels

- Vierogencontrole bevestigt complete custody, documenten, ontvanger en incidentstatus.
- Crewtoegang eindigt na debrief/afronding.
- Tijdelijke reis-, chat- en apparaatkopieën worden verwijderd.
- Klachten, claims of autoriteitsonderzoek activeren legal hold.
- Nazorg- en personeelswelzijnsgegevens blijven gescheiden van EMS-zaak.

Werkinstructie

1. Voer EMS-afsluitcheck uit.
2. Controleer custody, seal, documentversies en ontvangst.
3. Trek crew/partnerlinks en tijdelijke accounts in.
4. Pas retentie of legal hold toe.
5. Laat een bevoegde tweede persoon afsluiten en auditsteekproef plannen.

Verplichte vastlegging

EMS-afsluitformulier, toegangsintrekking, verwijdering, retentie/legal hold en vierogenhandtekening.

Direct escaleren of stoppen

Geen EMS-zaak sluiten bij custodygat, ontbrekende ontvangst, open privacyincident of onverklaarde persoonlijke bezitting.

DEEL IX

PERSONEELSPRIVACY

Werving, personeelsdossier, verzuim, monitoring, training en uitdiensttreding

95. Werving, selectie en VOG

Sollicitantgegevens worden alleen gebruikt voor objectieve selectie en worden beperkt tot wat voor de functie nodig is.

Kernregels

- Geen vragen naar gezondheid, zwangerschap, religie, politieke voorkeur of andere niet-relevante bijzondere gegevens.
- Referenties worden alleen met passende transparantie en bij voorkeur toestemming benaderd.
- VOG-status wordt geregistreerd; het document zelf alleen indien nodig en kort.
- Afgewezen sollicitatiegegevens worden in beginsel vier weken na einde procedure verwijderd, of maximaal één jaar met geldige toestemming.
- Selectietools en AI krijgen vooraf privacy- en discriminatietoets.

Werkinstructie

1. Bepaal functiecriteria en minimale gegevensset.
2. Informeer sollicitant over doelen, ontvangers en termijn.
3. Beperk toegang tot selectiecommissie.
4. Leg besluit feitelijk en professioneel vast.
5. Verwijder of vraag aparte toestemming voor talentpool.

Verplichte vastlegging

Vacature/privacyinformatie, sollicitatiedossier, referentie-/VOG-status, selectiebesluit, toestemming en verwijdering.

Direct escaleren of stoppen

Geen medische informatie of irrelevante privé-informatie uit sociale media in selectiedossier opnemen.

96. Personeelsdossier en toegang

Het personeelsdossier bevat noodzakelijke arbeids-, functie-, loon-, opleiding-, autorisatie- en gespreksgegevens en is gescheiden van operationele zaken en medische dossiers.

Kernregels

- HR-toegang is rolgebonden; leidinggevenden zien alleen wat voor hun taak nodig is.
- Loon/fiscale stukken kunnen andere wettelijke termijnen hebben dan algemene HR-notities.
- Subjectieve, beledigende of onbewezen observaties horen niet in het dossier.
- Medewerkerrechten en correcties worden via vaste procedure behandeld.
- Kopieën op lokale schijf of in persoonlijke mailbox zijn niet toegestaan.

Werkinstructie

1. Maak dossierstructuur per medewerker met documentcategorie en termijn.
2. Verifieer HR- en leidinggevenderechten.
3. Leg gesprekken feitelijk vast en deel concept waar passend.
4. Voer periodieke opschoning uit.
5. Sluit en archiveer bij uitdiensttreding volgens matrix.

Verplichte vastlegging

HR-dossierindex, autorisaties, documentversie, verzoek/correctie, opschoning en sluiting.

Direct escaleren of stoppen

Direct incidentmelding bij onbevoegde inzage, verkeerde loonstrookontvanger of HR-document in operationele groepsmap.

97. Ziekmelding, bedrijfsarts en medische scheiding

Werkgever en leidinggevende verwerken bij ziekte alleen noodzakelijke administratieve en inzetbaarheidsgegevens. Diagnose en medische behandeling blijven bij bedrijfsarts of arbodienst.

Kernregels

- Vraag naar verwachte duur, lopende afspraken, bereikbaarheid en mogelijke werkhervatting, niet naar diagnose.
- Medische documenten worden niet in algemeen personeelsdossier opgenomen.
- Bedrijfsarts deelt alleen functionele mogelijkheden en beperkingen voor re-integratie.
- Collega's ontvangen alleen noodzakelijke roosterinformatie.
- Blootstellings- en traumazorggegevens zijn extra beperkt.

Werkinstructie

1. Registreer ziekmelding via aangewezen kanaal en minimale velden.
2. Verwijs medische beoordeling naar arbodienst/bedrijfsarts.
3. Beperk toegang tot casemanager/HR volgens rol.
4. Deel functionele afspraken met leidinggevende.
5. Verwijder tijdelijke notities en bewaak wettelijke termijnen.

Verplichte vastlegging

Ziekmeldingsregister, contactafspraken, functionele terugkoppeling, toegangslog en verwijdering.

Direct escaleren of stoppen

Geen diagnose vragen of opnemen in rooster, e-mailonderwerp, teamchat of algemeen personeelsverslag.

98. Werknemersmonitoring en beoordeling

Prestatie- en gedragsbeoordeling steunt op transparante, relevante en verifieerbare informatie. GPS, camera, gespreksopnamen, systeemlogs of telematica worden niet sluipend als beoordelingsinstrument gebruikt.

Kernregels

- Doel, criteria, bronnen en bezwaarroute zijn vooraf bekend.
- Geen volledig geautomatiseerde negatieve beslissing.
- Context en hoor/wederhoor zijn verplicht bij mogelijke maatregel.
- Incidentele beveiligingslogs worden alleen voor personeelsdoel gebruikt na aparte juridische toets.
- Medezeggenschapsrechten worden gerespecteerd.

Werkinstructie

1. Bepaal rechtmatige en passende beoordelingsbronnen.
2. Informeer medewerker vooraf.
3. Controleer dat gegevens voor het betreffende doel zijn verzameld.
4. Bespreek context en laat correcties/zienswijze vastleggen.
5. Beperk bewaring en toegang van beoordelingsinformatie.

Verplichte vastlegging

Beoordelingscriteria, informatie, gegevensbronnen, hoor/wederhoor, besluit en bewaartermijn.

Direct escaleren of stoppen

Geen sanctie uitsluitend op GPS-afwijking, telematicascore, losse opname of ongeverifieerde systeemlog.

99. Geheimhouding, opleiding en veilige meldcultuur

Iedere medewerker en ingehuurde kracht krijgt vóór toegang passende geheimhouding, privacy- en beveiligingsinstructie en periodieke herhaling.

Kernregels

- Training is rolgericht voor meldkamer, chauffeurs, EMS, HR, administratie, IT en directie.
- Phishing, datalek, GPS, dossierdelen en EMS-waardigheid zijn verplichte onderwerpen.
- Kennis wordt getest; aanwezigheid alleen is onvoldoende.
- Fouten en bijna-incidenten worden direct gemeld zonder angst voor automatische bestraffing.
- Opzettelijk misbruik, verzwijgen of bewijsmanipulatie wordt afzonderlijk behandeld.

Werkinstructie

1. Voer basistraining uit vóór accountactivering.
2. Laat geheimhoudings- en ontvangstverklaring ondertekenen.
3. Test kennis met scenario’s en corrigeer hiaten.
4. Herhaal jaarlijks en na belangrijke wijziging/incident.
5. Blokkeer bevoegdheid bij verlopen verplichte training.

Verplichte vastlegging

Trainingsregister, toets, geheimhouding, autorisatieblokkering en hertraining.

Direct escaleren of stoppen

Geen toegang tot EMS, HR of beheeromgeving zonder geldige roltraining en geheimhouding.

100. Uitdiensttreding, dossierafsluiting en rechten

Bij einde dienstverband of opdracht worden toegang, apparatuur, sleutels, documenten en gegevenskopieën gecontroleerd ingetrokken en wordt het personeelsdossier volgens termijnen beheerd.

Kernregels

- Blokkeringstijd sluit aan op feitelijk einde of eerder risico.
- Zakelijke gegevens worden vóór afsluiting veilig overgedragen zonder privé-inhoud onnodig te doorzoeken.
- Doorsturen van mailbox wordt alleen beperkt, tijdelijk en transparant ingericht.
- Ex-medewerker behoudt rechten op eigen persoonsgegevens binnen wettelijke kaders.
- Geheimhouding blijft gelden na vertrek.

Werkinstructie

1. Start leaverchecklist met effectieve datum en risico.
2. Trek digitale/fysieke toegang en tokens in.
3. Neem apparaten, documenten, sleutels en betaalmiddelen in.
4. Archiveer noodzakelijke HR-stukken en verwijder overige data.
5. Bevestig afronding, resterende geheimhouding en contactroute.

Verplichte vastlegging

Leaverchecklist, blokkering, inname, gegevensoverdracht, retentie en exitbevestiging.

Direct escaleren of stoppen

Directe escalatie bij bulkdownload vóór vertrek, ontbrekend apparaat, gedeelde wachtwoorden of weigering tot gegevensinname.

DEEL X

BEHEERSING EN IMPLEMENTATIE

Training, audits, KPI's, managementreview, oefeningen, CAPA en livegang

101. Bewustwording en opleidingsprogramma

DriveBack onderhoudt een jaarlijks programma dat medewerkers leert veilig te handelen in de concrete 24/7 praktijk en niet alleen algemene regels te herkennen.

Kernregels

- Basistraining vóór toegang; roltraining vóór operationele autorisatie.
- Korte herhaling na incident, wijziging of waargenomen risico.
- Scenario's behandelen phishing, verkeerde ontvanger, GPS, EMS-custody, systeemuitval en privacyverzoek.
- Directie volgt bestuurlijke cyber- en privacytraining.
- Resultaten sturen verbeteracties en autorisatie.

Werkinstructie

1. Maak opleidingsmatrix per rol en risico.
2. Plan onboarding, jaarlijkse herhaling en oefeningen.
3. Toets kennis en praktische uitvoering.
4. Hertrain en beperk bevoegdheid bij onvoldoende resultaat.
5. Rapporteer deelname, trends en effectiviteit.

Verplichte vastlegging

Opleidingsmatrix, materiaalversie, aanwezigheid, toetsresultaat, hertraining en managementrapportage.

Direct escaleren of stoppen

Geen kritieke rol laten uitvoeren bij verlopen verplichte training of aantoonbaar onvoldoende kennis.

102. Interne audits en steekproeven

Audits toetsen of beleid, systemen en feitelijk gedrag overeenkomen en of maatregelen werkelijk effectief zijn.

Kernregels

- Auditprogramma is risicogebaseerd en dekt AVG, toegang, retentie, GPS, leveranciers, incidenten en herstel.
- Auditor beoordeelt niet uitsluitend eigen werk.
- Steekproef bevat Mobiliteit, EMS, COMBI, HR en incidentdossiers.
- Bevindingen zijn feitelijk, geclassificeerd en hebben eigenaar/deadline.
- Herstel wordt onafhankelijk geverifieerd.

Werkinstructie

1. Bepaal jaarlijkse scope op risico's en eerdere bevindingen.

2. Selecteer bewijs, interviews, systeemexports en dossiers.
3. Classificeer afwijking als observatie, minor, major of kritisch.
4. Laat proceseigenaar oorzaakanalyse en actieplan maken.
5. Verifieer effectiviteit en rapporteer aan directie.

Verplichte vastlegging

Auditplan, werkprogramma, steekproef, bevindingen, actieplan, verificatie en rapport.

Direct escaleren of stoppen

Kritische bevinding of herhaalde major wordt direct buiten reguliere auditcyclus geëscaleerd.

103. Toegangs-, retentie- en GPS-audits

Drie controles krijgen vaste frequentie vanwege hoge impact: autorisaties, automatische verwijdering en locatie-/monitoringgebruik.

Kernregels

- Toegangsreview: kritieke rollen per kwartaal, overige minimaal halfjaarlijks.
- Retentie: maandelijkse uitzonderingslijst en kwartaalsteekproef op werkelijk wissen.
- GPS: kwartaalcontrole op tracking buiten dienst, exports, toegang en automatische verwijdering.
- EMS-inzage: steekproef op toegewezen zaak en noodzaak.
- Bevindingen leiden tot intrekking, incidentbeoordeling en CAPA.

Werkinstructie

1. Exporteer actuele rechten, logins, retentie-uitzonderingen en GPS-raadplegingen.
2. Vergelijk met functie, actieve zaken, LIA/DPIA en matrix.
3. Onderzoek afwijkingen met eigenaar.
4. Corrigeer en beoordeel datalek/disciplinair risico.
5. Leg trend en herhaling voor aan management.

Verplichte vastlegging

Auditexports, vergelijking, afwijkingsdossier, correctie, incidentbesluit en trendrapport.

Direct escaleren of stoppen

Onbekend account, tracking na dienst of dossier dat na termijn zichtbaar blijft krijgt minimaal I2-beoordeling.

104. Leveranciersbeoordeling en assurance

Kritieke leveranciers worden vóór contract en periodiek beoordeeld op beveiliging, privacy, continuïteit, subverwerkers, incidentrespons en exit.

Kernregels

- Risicoklasse bepaalt diepgang en frequentie.
- Certificaten, SOC-rapporten of pentests worden op scope en actualiteit beoordeeld.
- Contractuele beloften worden vergeleken met configuratie en feitelijke dienstverlening.
- Incidenten, SLA-uitval en subverwerkerswijzigingen beïnvloeden score.
- Onvoldoende beheersing leidt tot verbeterplan, beperking of vervanging.

Werkinstructie

1. Classificeer leverancier op data, toegang, beschikbaarheid en vervangbaarheid.
2. Vraag en beoordeel bewijs.
3. Leg restrisico, contractmaatregelen en exit vast.

4. Monitor wijzigingen, incidenten en prestatie.
5. Herbeoordeel jaarlijks voor kritiek en minimaal tweejaarlijks voor middenrisico.

Verplichte vastlegging

Leveranciersscore, bewijs, contractafwijkingen, verbeterplan, acceptatie en exitbesluit.

Direct escaleren of stoppen

Geen verlenging van kritieke leverancier met openstaand hoog risico zonder directiebesluit en compensatie.

105. KPI's en KRI's

DriveBack gebruikt indicatoren om te sturen op risico en effectiviteit, niet om alleen aantallen te produceren.

Kernregels

- KPI's meten uitvoering, zoals tijdige review en training.
- KRI's waarschuwen voor risico, zoals mislukte back-ups, open kritieke patches en brede toegang.
- Definities, bron, eigenaar en rapportagefrequentie zijn vast.
- Indicatoren worden niet gemanipuleerd door incidenten niet te melden.
- Trends en drempels leiden tot concrete actie.

Werkinstructie

1. Stel beperkt kernset vast.
2. Automatiseer betrouwbare bron waar mogelijk.
3. Controleer datakwaliteit en context.
4. Rapporteer maandelijks/kwartaal en bespreek afwijkingen.
5. Pas maatregelen en indicatoren aan op nieuwe risico's.

Verplichte vastlegging

KPI/KRI-definities, dashboard, broncontrole, besluiten en acties.

Direct escaleren of stoppen

Rood drempelniveau zonder eigenaar en deadline wordt direct aan directie gemeld.

Aanbevolen kernindicatoren

Indicator	Doel	Frequentie	Eigenaar
Datalekbeoordeling binnen 24 uur	≥ 95%	Maandelijks	Privacycoördinator
AP-melding binnen 72 uur indien verplicht	100%	Per incident	Directie/privacy
Kritieke accounts met MFA	100%	Maandelijks	IT
Open kritieke toegangsafwijkingen	0	Maandelijks	IT/informatie-eigenaar
Kritieke back-up hersteltest geslaagd	100% per kwartaal	Kwartaal	IT/continuïteit
Ruwe GPS-data ouder dan termijn	0	Maandelijks	GPS-eigenaar
EMS-dossiers met complete custody	100%	Maandelijks steekproef	EMS-proceseigenaar
Kritieke leveranciers beoordeeld	100% jaarlijks	Kwartaal voortgang	Inkoop/privacy/IT
Verplichte training geldig	100% kritieke rollen	Maandelijks	HR
P0-CAPA over deadline	0	Maandelijks	Directie

106. Managementreview

De directie beoordeelt ten minste jaarlijks en voor kritieke onderwerpen per kwartaal of het privacy- en beveiligingssysteem geschikt, toereikend en effectief is.

Kernregels

- Input omvat risico's, incidenten, audits, KPI's, leveranciers, wetgeving, middelen, klachten en verbeteringen.
- Besluiten omvatten prioriteiten, budget, risicoacceptatie, beleid en verantwoordelijken.
- Openstaande acties uit vorige review worden gecontroleerd.
- Cbw-toepasselijkheid en schaalgroei zijn vaste agendapunten.
- Uitkomst wordt gecommuniceerd aan relevante rollen.

Werkinstructie

1. Verzamel gevalideerde input en openstaande acties.
2. Bespreek trends, restrisico en veranderingen.
3. Neem concrete besluiten met eigenaar en deadline.
4. Leg afwijkende meningen en risicoacceptatie vast.
5. Volg acties tot verificatie en sluiting.

Verplichte vastlegging

Agenda, input, notulen, besluiten, risicoacceptaties, budget en actielijst.

Direct escaleren of stoppen

Geen managementreview afsluiten zonder besluit over open kritieke risico's, hersteltests en incidentlessen.

107. CAPA en risicobehandeling

Corrective and Preventive Action zorgt dat afwijkingen niet alleen worden hersteld maar oorzaken aantoonbaar worden weggenomen.

Kernregels

- Iedere actie heeft risiconiveau, eigenaar, deadline en effectiviteitstest.
- P0 corrigeert direct of blokkeert de activiteit.
- Tijdelijke maatregel heeft expliciet vervolg naar structurele oplossing.
- Herhaald uitstel vereist nieuwe risicoacceptatie door hoger mandaat.
- Sluiting gebeurt pas na bewijs, niet op basis van mededeling.

Werkinstructie

1. Registreer bevinding, impact en tijdelijke beheersing.
2. Voer oorzaakanalyse uit.
3. Bepaal corrigerende en preventieve actie.
4. Implementeer en verzamel bewijs.
5. Test effectiviteit en laat onafhankelijk sluiten.

Verplichte vastlegging

CAPA-register, oorzaak, actie, bewijs, effectiviteitstest, restrisico en sluiting.

Direct escaleren of stoppen

P0 over deadline of ineffectieve herhaalde actie wordt direct door directie behandeld.

108. Oefeningen en testen

DriveBack oefent scenario's die 24/7 dienstverlening, privacy en informatiebeveiliging tegelijk raken.

Kernregels

- Minimaal jaarlijks: ransomware/systeemuitval, datalek, verloren apparaat, verkeerde ontvanger en EMS-custodyincident.
- Minimaal per kwartaal: hersteltest van kritieke data en handmatige fallback.
- Oefeningen gebruiken geen onnodige echte persoonsgegevens.
- Communicatie, besluitvorming, tijdlijnen en leveranciers worden meegenomen.
- Lessons learned leiden tot CAPA en herhaalde test.

Werkinstructie

1. Selecteer scenario, doelen, deelnemers en injects.
2. Leg nulmeting en succescriteria vast.
3. Voer oefening uit met waarnemers.
4. Debrief binnen twee werkdagen.
5. Implementeer verbeteringen en hertest kritieke tekortkomingen.

Verplichte vastlegging

Oefenplan, deelnemers, tijdlijn, observaties, evaluatie, CAPA en hertest.

Direct escaleren of stoppen

Een papieren oefening zonder daadwerkelijk herstel, accountblokkering of communicatie-test geldt niet als volledige technische test.

109. Implementatieroadmap en livegangcriteria

Formele ingebruikname volgt een aantoonbare GO/voorwaardelijke GO/NO-GO-beslissing. Open P0-punten blokkeren livegang.

Kernregels

- Beleid, rollen, contracten, systemen, training en incidentrespons worden als één geheel beoordeeld.
- Voorwaardelijke GO bevat beperkte scope, tijdelijke maatregelen, eigenaar en korte einddatum.
- Technische acceptatie omvat negatieve tests: onbevoegde toegang, verkeerde zaak en verlopen link.
- Juridische open punten zijn zichtbaar en worden niet verborgen in voetnoten.
- Na livegang volgt verhoogde monitoring en evaluatie.

Werkinstructie

1. Vul implementatiematrix in per maatregel en eigenaar.
2. Verzamel bewijs voor P0/P1 en voer acceptatietest uit.
3. Laat privacy, IT, proceseigenaar en directie beslissen.
4. Publiceer ingangsdatum en train gebruikers.
5. Voer 30-, 60- en 90-dagenreview uit.

Verplichte vastlegging

Implementatiematrix, testverslagen, open punten, risicobesluit, livegangverklaring en reviews.

Direct escaleren of stoppen

NO-GO bij ontbrekende MFA, onbekende incidentroute, ongeteste back-up, onbeperkte GPS-retentie, ontbrekende DPA of brede onbevoegde EMS-toegang.

DEEL XI

QUICK CARDS

Directe handelingskaarten voor meldkamer, planning, medewerkers, chauffeurs, EMS en leiding

DB-PIB-QC-01 | Mogelijk datalek

Gebruik deze kaart wanneer

Persoonsgegevens zijn kwijt, verkeerd verzonden, onbevoegd ingezien, gewijzigd, vernietigd of mogelijk buitgemaakt.

Direct doen

1. Stop de verspreiding of onveilige handeling zonder bewijs te wissen.
2. Meld direct via de 24/7-incidentroute en noteer kennisnametijd.
3. Trek link, sessie of toegang in indien veilig.
4. Bewaar e-mail, screenshot, log en betrokken document.
5. Volg instructies incidentleider en blijf bereikbaar.

Niet doen

- Niet zelf bepalen dat het “wel meevalt”.
- Niet wachten tot volgende werkdag.
- Niet alles verwijderen of apparaat resetten.
- Niet breed rondmailen wat er is gebeurd.
- Niet zelfstandig slachtoffers of media benaderen.

Registreren

Incidentnummer, tijd, melder, gegevens, betrokkenen, systeem, eerste maatregelen en ontvangers.

Escalatie

Direct I3/I4 bij gezondheidsgegevens, EMS, identiteitsdocumenten, grote aantallen, actieve publicatie of afpersing.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-02 | Verkeerde e-mail of bijlage

Gebruik deze kaart wanneer

Een bericht, link of bijlage is naar de verkeerde ontvanger gestuurd of bevat meer gegevens dan bedoeld.

Direct doen

1. Meld direct intern.
2. Trek deellink en eventuele sessies in.
3. Verifieer via bekende route wie de ontvanger is.
4. Vraag na akkoord incidentleider verwijdering en bevestiging.
5. Bewaar verzendlog, bericht en relevante toegangsgegevens.

Niet doen

- Niet alleen “recall” gebruiken en aannemen dat het opgelost is.
- Niet opnieuw het gevoelige document sturen ter uitleg.
- Niet vanaf privételefoon contact opnemen.
- Niet kennisnametijd aanpassen.

Registreren

E-mailadres, onderwerp, bijlagen, tijd, toegang/download, intrekking, ontvangerreactie.

Escalatie

Direct privacycoördinator bij ID, gezondheid, GPS, EMS of meerdere betrokkenen.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-03 | Verloren of gestolen apparaat

Gebruik deze kaart wanneer

Zakelijke telefoon, laptop, tablet, USB, papier of sleutel met toegang tot DriveBack-informatie is zoek of gestolen.

Direct doen

1. Bel direct de incidentroute.
2. Geef apparaat, gebruiker, laatste locatie/tijd en mogelijke data door.
3. Laat account/sessies blokkeren en MDM-locate/wipe uitvoeren.
4. Wijzig relevante credentials en tokens.
5. Doe aangifte wanneer incidentleider dit bepaalt.

Niet doen

- Niet zelf op gevaarlijke locatie terughalen.
- Niet dagen zoeken vóór melden.
- Niet vergeten dat papieren dossiers en sleutels ook incident zijn.
- Niet vanaf onbeveiligd toestel inloggen om te controleren.

Registreren

Assetnummer, encryptie/MDM-status, data, laatste gebruik, blokkering/wipe, aangifte.

Escalatie

I3/I4 als encryptie ontbreekt, EMS/HR-data lokaal stond of actieve sessie niet kan worden ingetrokken.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-04 | Verdachte e-mail, MFA of account

Gebruik deze kaart wanneer

Onverwachte link, bijlage, MFA-prompt, wachtwoordreset, mailboxregel of loginwaarschuwing.

Direct doen

1. Klik niet en keur MFA niet goed.
2. Meld bericht via beveiligingsroute.
3. Bij al geklikt/ingevoerd: meld dit direct en verbreek zo nodig netwerk.
4. Laat sessies/tokens blokkeren en mailboxregels controleren.
5. Volg resetinstructie via bekende IT-route.

Niet doen

- Niet schamen of verzwijgen.
- Niet alleen wachtwoord wijzigen zonder sessiecontrole.
- Niet antwoorden op verdachte afzender.
- Niet screenshot met gevoelige inhoud in teamchat delen.

Registreren

Afzender, onderwerp, tijd, link/domein, handeling, apparaat, MFA/logins.

Escalatie

I3/I4 bij beheerdersaccount, financiële fraude, exfiltratie of ransomware-indicatie.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-05 | Systeemuitval of ransomware

Gebruik deze kaart wanneer

Dossier, telefonie, AFAS, GPS, e-mail of netwerk is niet beschikbaar, bestanden zijn versleuteld of ransom note verschijnt.

Direct doen

1. Stop gebruik van getroffen systeem en isoleer apparaat indien geïnstrueerd.
2. Activeer 24/7 incident- en continuïteitsroute.
3. Start handmatige intake/fallback met unieke noodzaaknummers.
4. Bewaar foutmelding en tijd; maak geen herinstallatie.
5. Reconcilieer noodregistratie pas na herstelvrijgave.

Niet doen

- Niet betalen of onderhandelen.
- Niet USB/back-up aansluiten.
- Niet doorwerken in onbekende privétools.
- Niet aannemen dat een reboot veilig is.

Registreren

Starttijd, systemen, impact, handmatige dossiers, foutmelding, acties en hersteltijd.

Escalatie

Automatisch I4 bij ransomware of uitval van meldkamer/EMS-bronregistratie zonder werkbare fallback.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-06 | Onbevoegde dossierinzage of bulkexport

Gebruik deze kaart wanneer

Een gebruiker ziet dossiers buiten zijn taak, exporteert grote hoeveelheden of een ex-medewerkeraccount is actief.

Direct doen

1. Meld direct en noteer account, tijd en waarneming.
2. Laat toegang tijdelijk blokkeren zonder logs te wijzigen.
3. Beveilig exportbestanden en deelhistorie.
4. Controleer rol, zaaktoewijzing en logins.
5. Volg incidentleider voor hoor/wederhoor en datalekbeoordeling.

Niet doen

- Niet zelf de gebruiker beschuldigen in groepschat.
- Niet logs verwijderen.
- Niet export openen/kopiëren zonder noodzaak.
- Niet alleen rechten aanpassen en incident sluiten.

Registreren

Account, dossiers, acties, exportgrootte, locatie, device, reden/verklaring.

Escalatie

I3/I4 bij EMS, HR, gezondheidsgegevens, langdurige toegang of externe overdracht.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-07 | GPS volgt buiten dienst of verkeerde zaak

Gebruik deze kaart wanneer

Tracking blijft actief na dienst, toont verkeerde chauffeur/voertuig/zaak of is zichtbaar voor onbevoegden.

Direct doen

1. Stop of ontkoppel tracking indien veilig.
2. Meld incident met zaak, voertuig, gebruiker en tijdvenster.
3. Bewaar relevante logs en screenshots beperkt.
4. Controleer wie toegang had en of data is geëxporteerd.
5. Corrigeer koppeling en verwijder onrechtmatige data na besluit.

Niet doen

- Niet gebruiken voor personeelsbeoordeling.
- Niet hele route delen in chat.
- Niet stilzwijgend corrigeren zonder incidentregistratie.
- Niet tracking opnieuw activeren zonder test.

Registreren

Trackingvenster, personen/voertuig, viewers, exports, oorzaak en verwijdering.

Escalatie

Privacycoördinator en leidinggevende; I3 bij structurele of heimelijke tracking.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-08 | Privacyverzoek

Gebruik deze kaart wanneer

Iemand vraagt om inzage, correctie, verwijdering, bezwaar, beperking of kopie van eigen persoonsgegevens.

Direct doen

1. Registreer ontvangstdatum en stuur ontvangstbevestiging.
2. Stuur verzoek naar privacycontact; ga niet inhoudelijk improviseren.
3. Verifieer identiteit proportioneel via vast proces.
4. Blokkeer ongecontroleerde verwijdering en beoordeel legal hold.
5. Bewaar alle zoek- en beslisstappen.

Niet doen

- Niet standaard volledige ID-kopie vragen.
- Niet verzoek negeren omdat het via e-mail/telefoon komt.
- Niet gegevens van anderen meesturen.
- Niet termijn laten verlopen zonder gemotiveerde communicatie.

Registreren

Verzoek, datum, identiteit, scope, systemen, besluit en uitvoering.

Escalatie

Direct escaleren bij EMS-dossier met meerdere betrokkenen, claim, toezichthouder of termijn <5 werkdagen.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-09 | EMS-identiteit, seal of custody klopt niet

Gebruik deze kaart wanneer

Naam/document/kistlabel/seal wijkt af, custody is onvolledig of ontvanger is niet bevoegd.

Direct doen

1. Zet transport/overdracht onmiddellijk op HOLD.
2. Waarborg waardige en veilige fysieke situatie.
3. Bel senior EMS-planner en incidentleider.
4. Voer vierogencontrole uit op documenten, seal en partijen.
5. Bewaar originele informatie en maak geen onzichtbare correctie.

Niet doen

- Niet raden of “waarschijnlijk goed” accepteren.
- Niet openen, resealen of verder overdragen zonder bevoegd besluit.
- Niet nabestaanden individueel benaderen zonder aangewezen communicator.
- Niet foto’s breed delen.

Registreren

Alle identificatoren, custody, seal, locatie, partijen, tijdlijn en beslissingen.

Escalatie

Automatisch I4; directie, EMS-leiding, privacy/juridisch en waar nodig autoriteiten.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-10 | Ongepaste foto of publicatie

Gebruik deze kaart wanneer

Een EMS-, klant-, personeels- of voertuigbeeld staat op privételefoon, sociale media, openbare link of verkeerde omgeving.

Direct doen

1. Meld direct en beveilig URL/screenshot als bewijs.
2. Laat publicatie/link verwijderen of intrekken.
3. Bepaal bereik, downloads, deelacties en betrokkenen.
4. Blokkeer account/apparaat indien nodig.
5. Voer datalek-, waardigheids- en arbeidsrechtelijke beoordeling uit.

Niet doen

- Niet reageren in openbare comments.
- Niet beeld verder delen om te vragen wie het heeft geplaatst.
- Niet alleen verwijderen zonder bewijs.
- Niet zelf media of nabestaanden bellen.

Registreren

URL, platform, account, tijd, bereik, beeldcategorie, verwijdering en bewijs.

Escalatie

I4 bij herkenbaar beeld overledene; I3 bij gezondheids-/ID-/personeelsbeeld of grote verspreiding.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-11 | Buitenlandse partner vraagt extra documenten

Gebruik deze kaart wanneer

Een onbekende of gewijzigde buitenlandse ontvanger vraagt paspoort, medische gegevens, EMS-documenten, betaling of volledige zaak.

Direct doen

1. Pauzeer verzending.
2. Verifieer partner via bestaand nummer, opdrachtgever of officiële bron.
3. Bepaal minimale noodzakelijke documenten en doorgiftebasis.
4. Gebruik beveiligd kanaal en registreer verzending.
5. Escaleren bij druk, afwijkende rekening of ongewoon verzoek.

Niet doen

- Niet antwoorden via alleen het nieuwe e-mailadres.
- Niet volledige zaak “om tijd te winnen” sturen.
- Niet bankrekeningwijziging accepteren zonder vierogen/tweede kanaal.
- Niet privécloud of publieke link gebruiken.

Registreren

Partner, land, rol, verzoek, verificatie, doorgiftebasis, verzonden set en ontvangst.

Escalatie

I3 bij mogelijke fraude, onbevoegde doorgifte buiten EER of reeds verzonden gevoelige data.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DB-PIB-QC-12 | Dossier afsluiten

Gebruik deze kaart wanneer

Operationele overdracht is gereed en de zaak moet worden gesloten.

Direct doen

1. Controleer verplichte documenten, overdracht, custody en incidentstatus.
2. Verwijder tijdelijke chat-, download- en apparaatkopieën.
3. Trek deel-links, crew- en partnerrechten in.
4. Stel bewaartermijn of legal hold vast.
5. Laat EMS/COMBI vierogen afsluiten.

Niet doen

- Niet sluiten met open incident, claim of onbekende ontvanger.
- Niet ruwe GPS, ID-kopie of opname onbeperkt laten staan.
- Niet lokale mappen vergeten.
- Niet ontbrekende documenten stilzwijgend markeren als compleet.

Registreren

Afsluitcheck, verwijderingen, rechten, retentie/legal hold, reviewer en datum.

Escalatie

Escaleren bij custodygat, ontbrekende overdracht, open datalek of systeem dat verwijdering niet ondersteunt.

Bij acuut gevaar: bel 112. Intern 24/7 incidentnummer: [IN TE VULLEN].

DEEL XII

REGISTERS EN FORMULIEREN

Direct bruikbare sjablonen voor implementatie, bewijs, incidenten en audits

DB-PIB-F01 | Implementatie- en livegangbesluit

Gebruik dit formulier om per proces of systeem formeel GO, voorwaardelijke GO of NO-GO vast te leggen.

Gebruik

Open P0-punten blokkeren livegang. Een voorwaardelijke GO vermeldt altijd scope, compensatie, eigenaar en einddatum.

Proces / systeem	[IN TE VULLEN]
Dienststroom	☐ DriveBack Mobiliteit ☐ EMS ☐ Beide ☐ HR/Bedrijfsvoering
Proceseigenaar	[IN TE VULLEN]
Systeemeigenaar	[IN TE VULLEN]
Verwerkingsregistercode	[IN TE VULLEN]
Privacyrol	☐ Verantwoordelijke ☐ Verwerker ☐ Gezamenlijk ☐ N.v.t.
Grondslag / uitzondering	[IN TE VULLEN]
DPIA/LIA-status	☐ Niet vereist ☐ Gereed ☐ Openstaand
DPA / contractstatus	☐ Gereed ☐ Openstaand ☐ N.v.t.
MFA en autorisaties getest	☐ Ja ☐ Nee
Logging en retentie getest	☐ Ja ☐ Nee
Back-up/herstel of fallback getest	☐ Ja ☐ Nee
Open P0-punten	[IN TE VULLEN]
Open P1-punten en deadline	[IN TE VULLEN]
Besluit	☐ GO ☐ VOORWAARDELIJKE GO ☐ NO-GO
Voorwaarden / restrisico	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F02 | Register van verwerkingsactiviteiten

Eén formulier per verwerking. Neem de regel vervolgens op in het centrale verwerkingsregister.

Gebruik
Vermijd generieke omschrijvingen. Noem werkelijke systemen, ontvangers en termijnen.

Registercode	[IN TE VULLEN]
Naam verwerking	[IN TE VULLEN]
Proceseigenaar	[IN TE VULLEN]
Privacyrol DriveBack	☐ Verantwoordelijke ☐ Verwerker ☐ Gezamenlijk
Doel(en)	[IN TE VULLEN]
Categorieën betrokkenen	[IN TE VULLEN]
Persoonsgegevens	[IN TE VULLEN]
Bijzonder/strafrechtelijk	[IN TE VULLEN / N.v.t.]
Grondslag en eventuele uitzondering	[IN TE VULLEN]
Bronnen	[IN TE VULLEN]
Ontvangers / categorieën	[IN TE VULLEN]
Systemen en locaties	[IN TE VULLEN]
Doorgifte buiten EER	☐ Nee ☐ Ja, land/mechanisme: [IN TE VULLEN]
Bewaartermijn en starttrigger	[IN TE VULLEN]
Beveiligingsmaatregelen	[IN TE VULLEN]
DPIA/LIA	[IN TE VULLEN]
Laatste review / volgende review	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F03 | Dataflow- en systeeminventarisatie

Breng de volledige gegevensstroom in kaart, inclusief tijdelijke kanalen, exports en leveranciers.

Gebruik
Controleer ook e-mail, WhatsApp, voertuigapps, GPS-platform, printers, scanners, hotel-/reisportalen en papieren sets.

Proces / use case	[IN TE VULLEN]
Startpunt / bron	[IN TE VULLEN]
Ontvangen gegevens	[IN TE VULLEN]
Kanaal / formulier	[IN TE VULLEN]
Bronregistratie	[IN TE VULLEN]
Koppelingen / API's	[IN TE VULLEN]
Tijdelijke opslag / downloads	[IN TE VULLEN]
Interne rollen	[IN TE VULLEN]
Externe ontvangers	[IN TE VULLEN]
Landen / hosting / support	[IN TE VULLEN]
Classificatie	☐ Openbaar ☐ Intern ☐ Vertrouwelijk ☐ Zeer vertrouwelijk
Uitvoer / rapportage	[IN TE VULLEN]
Verwijderroute	[IN TE VULLEN]
Onbekende stromen / shadow IT	[IN TE VULLEN]
Acties en eigenaar	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F04 | Privacyrolbeoordeling

Bepaal of DriveBack verwerkingsverantwoordelijke, verwerker, gezamenlijk verantwoordelijke of zelfstandige ontvanger is.

Gebruik
De feitelijke situatie is doorslaggevend; een contractlabel alleen bepaalt de AVG-rol niet.

Proces / relatie	[IN TE VULLEN]
Wederpartij	[IN TE VULLEN]
Wie bepaalt doel?	[IN TE VULLEN]
Wie bepaalt essentiële middelen?	[IN TE VULLEN]
Wie geeft instructies?	[IN TE VULLEN]
Kan DriveBack gegevens voor eigen doel gebruiken?	☐ Nee ☐ Ja, toelichting: [IN TE VULLEN]
Wie informeert betrokkenen?	[IN TE VULLEN]
Wie behandelt rechten?	[IN TE VULLEN]
Wie beslist over bewaartermijn?	[IN TE VULLEN]
Wie meldt datalek aan wie?	[IN TE VULLEN]
Conclusie rol	☐ Verantwoordelijke ☐ Verwerker ☐ Gezamenlijk ☐ Zelfstandige ontvanger
Benodigde overeenkomst	☐ DPA ☐ Gegevensdeling ☐ Gezamenlijke regeling ☐ Dienstverlening
Motivering	[IN TE VULLEN]
Herbeoordelingsmoment	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F05 | Grondslagen- en gevoelige-gegevenscheck

Leg per doel vast op welke grondslag persoonsgegevens worden verwerkt en welke aanvullende uitzondering geldt voor bijzondere gegevens.

Gebruik

Toestemming is geen standaardoplossing. Bijzondere gegevens vereisen naast de gewone grondslag een passende uitzondering.

Verwerking / doel	[IN TE VULLEN]
Gegevenscategorieën	[IN TE VULLEN]
Betrokkenen	[IN TE VULLEN]
Gewone grondslag	☐ Overeenkomst ☐ Wet ☐ Gerechtvaardigd belang ☐ Vitaal belang ☐ Toestemming ☐ Publieke taak
Concrete motivering / wetsartikel	[IN TE VULLEN]
Bijzondere persoonsgegevens	☐ Nee ☐ Ja: [IN TE VULLEN]
Aanvullende uitzondering	[IN TE VULLEN / N.v.t.]
Strafrechtelijke gegevens	☐ Nee ☐ Ja, wettelijke basis: [IN TE VULLEN]
Minder ingrijpend alternatief	[IN TE VULLEN]
Minimale gegevensset	[IN TE VULLEN]
Privacyinformatie aangepast	☐ Ja ☐ Nee
Register aangepast	☐ Ja ☐ Nee
Besluit / voorwaarden	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F06 | LIA - gerechtvaardigd belang

Gebruik vóór verwerking op grond van gerechtvaardigd belang, onder meer bij GPS, beveiligingslogging en sommige fraudepreventie.

Gebruik

Een algemene verwijzing naar “bedrijfsbelang” is onvoldoende. Beschrijf alternatieven, impact en mitigatie.

Use case	[IN TE VULLEN]
Gerechtvaardigd belang	[IN TE VULLEN]
Wie heeft dit belang?	[IN TE VULLEN]
Is het belang rechtmatig en concreet?	[IN TE VULLEN]
Noodzakelijkheid	[IN TE VULLEN]
Minder ingrijpende alternatieven	[IN TE VULLEN]
Betrokkenen / kwetsbaarheid	[IN TE VULLEN]
Redelijke verwachtingen	[IN TE VULLEN]
Mogelijke gevolgen	[IN TE VULLEN]
Maatregelen	[IN TE VULLEN]
Bezwaarroute	[IN TE VULLEN]
Uitkomst belangenafweging	☐ Toelaatbaar ☐ Voorwaardelijk ☐ Niet toelaatbaar
Restrisico / reviewdatum	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F07 | DPIA-screening

Bepaal vóór een nieuwe of gewijzigde verwerking of een volledige DPIA verplicht of verstandig is.

Gebruik
Bij twijfel en meerdere risicocriteria: voer een volledige DPIA uit vóór aanschaf of livegang.

Proces / systeem	[IN TE VULLEN]
Nieuwe technologie	☐ Nee ☐ Ja
Stelselmatige observatie / GPS / monitoring	☐ Nee ☐ Ja
Bijzondere of zeer gevoelige gegevens	☐ Nee ☐ Ja
Kwetsbare betrokkenen	☐ Nee ☐ Ja
Grote schaal / veel betrokkenen	☐ Nee ☐ Ja
Koppeling datasets / profilering	☐ Nee ☐ Ja
Besluitvorming met grote gevolgen	☐ Nee ☐ Ja
Doorgifte / complexe keten	☐ Nee ☐ Ja
Belemmering rechten of dienstafhankelijkheid	☐ Nee ☐ Ja
Waarschijnlijk hoog privacyrisico	☐ Nee ☐ Ja / onzeker
Conclusie	☐ Geen DPIA ☐ Vrijwillige DPIA ☐ Verplichte DPIA
Motivering en maatregelen vóór livegang	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F08 | DPIA - volledige beoordeling

Volledige analyse van verwerking, noodzaak, risico's voor betrokkenen, maatregelen en restrisico.

Gebruik

Voeg risico-overzicht en maatregelplan als bijlage toe. Restrisico hoog zonder voldoende maatregel kan voorafgaande raadpleging vereisen.

DPIA-code / versie	[IN TE VULLEN]
Proces, systeem en eigenaar	[IN TE VULLEN]
Beschrijving verwerking en dataflow	[IN TE VULLEN]
Doel, grondslag en noodzaak	[IN TE VULLEN]
Betrokkenen en gegevens	[IN TE VULLEN]
Omvang, frequentie, duur en landen	[IN TE VULLEN]
Redelijke verwachtingen	[IN TE VULLEN]
Risico's voor rechten en vrijheden	[IN TE VULLEN]
Bestaande maatregelen	[IN TE VULLEN]
Aanvullende maatregelen en eigenaar	[IN TE VULLEN]
Restrisico per hoofdscenario	[IN TE VULLEN]
Advies privacy/FG	[IN TE VULLEN]
Medezeggenschap / betrokkenen geraadpleegd	[IN TE VULLEN]
Voorafgaande raadpleging AP nodig	☐ Nee ☐ Ja
Bestuursbesluit	☐ GO ☐ Voorwaardelijk ☐ NO-GO
Reviewdatum / wijzigingstriggers	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F09 | Privacyverklaring- en transparantiecheck

Controleer of betrokkenen juist, volledig en tijdig worden geïnformeerd.

Gebruik
De websiteverklaring alleen is niet genoeg voor personeelsmonitoring, GPS of specifieke EMS-intake.

Doelgroep	☐ Klant ☐ Website ☐ Sollicitant ☐ Medewerker ☐ GPS ☐ EMS ☐ Anders
Verklaring / versie / datum	[IN TE VULLEN]
Verantwoordelijke en contact	[IN TE VULLEN]
Doelen en grondslagen compleet	☐ Ja ☐ Nee
Gegevenscategorieën begrijpelijk	☐ Ja ☐ Nee
Ontvangers en leveranciers	[IN TE VULLEN]
Doorgiften buiten EER	[IN TE VULLEN / N.v.t.]
Bewaartermijnen / criteria	[IN TE VULLEN]
Rechten en klacht AP	☐ Compleet ☐ Aanpassen
Verplichte/optionele gegevens en gevolgen	[IN TE VULLEN]
Automatisering / monitoring	[IN TE VULLEN / N.v.t.]
Moment en kanaal verstrekking	[IN TE VULLEN]
Taalniveau / toegankelijkheid getest	☐ Ja ☐ Nee
Publicatie- en wijzigingsplan	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F10 | Verzoek van betrokkene

Registreer inzage, correctie, verwijdering, beperking, bezwaar, overdraagbaarheid of informatieverzoek.

Gebruik
In beginsel binnen één maand reageren. Verlenging wordt vóór het einde van de eerste maand gemotiveerd meegedeeld.

Verzoeknummer	[IN TE VULLEN]
Datum/tijd ontvangst	[IN TE VULLEN]
Naam / contact	[IN TE VULLEN]
Type verzoek	☐ Inzage ☐ Correctie ☐ Verwijdering ☐ Beperking ☐ Bezwaar ☐ Overdracht ☐ Informatie
Dossiers / periode / scope	[IN TE VULLEN]
Identiteitsverificatie	[IN TE VULLEN]
Ontvangstbevestiging datum	[IN TE VULLEN]
Uiterste reactiedatum	[IN TE VULLEN]
Systemen en verwerkers doorzocht	[IN TE VULLEN]
Gegevens van derden / redactie	[IN TE VULLEN]
Legal hold / uitzondering	[IN TE VULLEN / N.v.t.]
Besluit	☐ Volledig ☐ Gedeeltelijk ☐ Afgewezen
Uitvoering / verstrekte informatie	[IN TE VULLEN]
Reactiedatum / afsluiting	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F11 | Proportionele identiteitsverificatie

Bepaal de minst ingrijpende betrouwbare methode om een verzoeker of ontvanger te verifiëren.

Gebruik
Vraag niet standaard een volledige identiteitskopie. Leg alleen noodzakelijke kenmerken en verificatiestatus vast.

Verzoek / overdracht	[IN TE VULLEN]
Bekende relatie / zaak	[IN TE VULLEN]
Risico bij verkeerde identiteit	[IN TE VULLEN]
Bestaand geverifieerd kanaal beschikbaar	☐ Ja ☐ Nee
Controle via dossierkennis	[IN TE VULLEN]
Tweede kanaal / terugbelprocedure	[IN TE VULLEN]
Beperkte documentcontrole nodig	☐ Nee ☐ Ja, welke kenmerken: [IN TE VULLEN]
Volledige kopie noodzakelijk	☐ Nee ☐ Ja, motivering: [IN TE VULLEN]
Afscherming / watermerk	[IN TE VULLEN]
Verwijderdatum verificatiekopie	[IN TE VULLEN]
Conclusie identiteit	☐ Bevestigd ☐ Onvoldoende ☐ Escalatie

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F12 | Privacyklacht en onderzoek

Gebruik bij klacht over verwerking, toegang, GPS, communicatie, foto, retentie of uitoefening van rechten.

Gebruik
Verwijder geen dossierinformatie voordat legal-hold- en onderzoeksbeoordeling zijn afgerond.

Klachtnummer	[IN TE VULLEN]
Ontvangstdatum / kanaal	[IN TE VULLEN]
Klager / contact	[IN TE VULLEN]
Onderwerp / betrokken proces	[IN TE VULLEN]
Gewenste oplossing	[IN TE VULLEN]
Onderzoeker	[IN TE VULLEN]
Bewijs veiliggesteld	[IN TE VULLEN]
Datalek / incident mogelijk	☐ Nee ☐ Ja, incidentnummer: [IN TE VULLEN]
Feiten en tijdlijn	[IN TE VULLEN]
Beoordeling rechtmatigheid/beveiliging	[IN TE VULLEN]
Hoor en wederhoor	[IN TE VULLEN]
Besluit en herstel	[IN TE VULLEN]
Communicatiedatum	[IN TE VULLEN]
CAPA / managementreview	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F13 | Autorisatieaanvraag

Formele aanvraag voor nieuwe of gewijzigde systeem- en dossierrechten.

Gebruik

Extra export-, verwijder- en beheerrechten worden afzonderlijk gemotiveerd en zijn niet onderdeel van een standaardrol.

Aanvraagnummer	[IN TE VULLEN]
Medewerker / extern	[IN TE VULLEN]
Werkgever / leverancier	[IN TE VULLEN]
Functie en team	[IN TE VULLEN]
Ingangsdatum / einddatum	[IN TE VULLEN]
Systemen / modules	[IN TE VULLEN]
Dienststroom	☐ Mobiliteit ☐ EMS ☐ COMBI ☐ HR ☐ Financieel ☐ IT
Rechten	☐ Lezen ☐ Aanmaken ☐ Wijzigen ☐ Export ☐ Verwijderen ☐ Beheer
Zakelijke noodzaak	[IN TE VULLEN]
Classificatie	☐ Intern ☐ Vertrouwelijk ☐ Zeer vertrouwelijk
Training / geheimhouding geldig	☐ Ja ☐ Nee
MFA / apparaat compliant	☐ Ja ☐ Nee
Leidinggevende goedkeuring	[IN TE VULLEN]
Informatie-eigenaar goedkeuring	[IN TE VULLEN]
Technisch uitgevoerd / getest	[IN TE VULLEN]
Reviewdatum	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F14 | Periodieke toegangsreview

Controleer accounts, rollen, groepen, laatste login, zaaktoegang en uitzonderingen.

Gebruik

Laat de review bevestigen door leidinggevende én informatie-eigenaar; de technische uitvoerder sluit niet zelfstandig zijn eigen bevindingen.

Reviewperiode	[IN TE VULLEN]
Systeem / omgeving	[IN TE VULLEN]
Reviewer	[IN TE VULLEN]
Aantal accounts	[IN TE VULLEN]
Inactieve accounts	[IN TE VULLEN]
Ex-medewerker / externe accounts	[IN TE VULLEN]
Beheer- en break-glassaccounts	[IN TE VULLEN]
EMS-/HR-toegang steekproef	[IN TE VULLEN]
Bulkexport / afwijkende inzage	[IN TE VULLEN]
Gedeelde / onbekende accounts	[IN TE VULLEN]
Besluiten per afwijking	[IN TE VULLEN]
Intrekkingen / wijzigingen	[IN TE VULLEN]
Mogelijk incident	☐ Nee ☐ Ja, nummer: [IN TE VULLEN]
Volgende review	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F15 | Joiner-Mover-Leaverchecklist

Gebruik bij indiensttreding, functiewijziging, tijdelijke inzet, uitdiensttreding of acute blokkering.

Gebruik
Bij mover: oude rechten eerst intrekken en daarna nieuwe rechten activeren. Bij risico: onmiddellijk blokkeren.

Type	☐ Joiner ☐ Mover ☐ Leaver ☐ Acute blokkering
Naam / personeelsnummer	[IN TE VULLEN]
Functie oud / nieuw	[IN TE VULLEN]
Effectieve datum en tijd	[IN TE VULLEN]
Contract / identiteit geverifieerd	☐ Ja ☐ Nee
Geheimhouding / training	[IN TE VULLEN]
Accounts en groepen	[IN TE VULLEN]
MFA / tokens / wachtwoordmanager	[IN TE VULLEN]
Apparaten / MDM	[IN TE VULLEN]
Voertuig-/GPS-apps	[IN TE VULLEN]
Fysieke passen / sleutels	[IN TE VULLEN]
Mailbox / dossiers / gedeelde mappen	[IN TE VULLEN]
API / service / externe portals	[IN TE VULLEN]
Inname / overdracht zakelijke data	[IN TE VULLEN]
Technische controle afgerond	[IN TE VULLEN]
Afwijkingen / incident	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F16 | Privileged access / break-glassgebruik

Registreer tijdelijke beheer- of noodtoegang en controleer de sessie achteraf.

Gebruik
Noodtoegang wordt niet gebruikt voor gemak of regulier beheer. Gebruik genereert een onafhankelijke review.

Ticket / incidentnummer	[IN TE VULLEN]
Gebruiker / leverancier	[IN TE VULLEN]
Beheeraccount	[IN TE VULLEN]
Systeem / scope	[IN TE VULLEN]
Zakelijke/noodzaakreden	[IN TE VULLEN]
Start / geplande eindtijd	[IN TE VULLEN]
Goedkeurder 1	[IN TE VULLEN]
Goedkeurder 2 / noodbeheer	[IN TE VULLEN]
MFA / sessieregistratie	[IN TE VULLEN]
Uitgevoerde acties	[IN TE VULLEN]
Inhoudelijke dossierinzage nodig	☐ Nee ☐ Ja, motivering: [IN TE VULLEN]
Eindtijd / rechten ingetrokken	[IN TE VULLEN]
Logreview door	[IN TE VULLEN]
Sleutel/token geroteerd	[IN TE VULLEN]
Afwijking / incident	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F17 | Assetregister en lifecycle

Registreer hardware, software, cloudservice, voertuig-/GPS-systeem, koppeling of papieren archief.

Gebruik
Ieder operationeel asset heeft een eigenaar, updatepad, incidentcontact en veilige afvoerroute.

Asset-ID	[IN TE VULLEN]
Naam / type / model	[IN TE VULLEN]
Serienummer / tenant / URL	[IN TE VULLEN]
Bedrijfseigenaar	[IN TE VULLEN]
Technisch eigenaar	[IN TE VULLEN]
Gebruiker / locatie	[IN TE VULLEN]
Processen / data	[IN TE VULLEN]
Classificatie / kritikaliteit	[IN TE VULLEN]
Leverancier / contract	[IN TE VULLEN]
Hosting / landen	[IN TE VULLEN]
Versie / support-einde	[IN TE VULLEN]
Encryptie / MDM / patchstatus	[IN TE VULLEN]
Back-up / herstel	[IN TE VULLEN]
Risico / afhankelijkheden	[IN TE VULLEN]
Lifecycle-status	☐ Actief ☐ Reserve ☐ Uitfaseren ☐ Afgevoerd
Afvoer / vernietigingsbewijs	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F18 | Leveranciers- en verwerkersbeoordeling

Beoordeel een leverancier vóór contract, periodiek en na materiële wijziging of incident.

Gebruik
Een certificaat is ondersteunend bewijs; controleer scope, actualiteit en feitelijke configuratie.

Leverancier / dienst	[IN TE VULLEN]
Bedrijfseigenaar	[IN TE VULLEN]
Risicoklasse	☐ Laag ☐ Midden ☐ Kritiek
Privacyrol	[IN TE VULLEN]
Persoonsgegevens / classificatie	[IN TE VULLEN]
Beschikbaarheid / RTO/RPO	[IN TE VULLEN]
Hosting / supportlanden	[IN TE VULLEN]
Subverwerkers	[IN TE VULLEN]
DPA / contract / auditrechten	[IN TE VULLEN]
MFA / encryptie / logging	[IN TE VULLEN]
Patch / kwetsbaarheid / pentest	[IN TE VULLEN]
Datalekmeldtermijn en contact	[IN TE VULLEN]
Back-up / continuïteit / exit	[IN TE VULLEN]
Certificaten / assurance en scope	[IN TE VULLEN]
Open risico's / maatregelen	[IN TE VULLEN]
Besluit	☐ Goedkeuren ☐ Voorwaardelijk ☐ Afwijzen
Volgende review	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F19 | Verwerkersovereenkomst-checklist

Controleer of de verwerkersovereenkomst aansluit op artikel 28 AVG en de feitelijke dienstverlening.

Gebruik
Gebruik geen generieke DPA die niet overeenkomt met werkelijke data, subverwerkers, locaties en incidentroute.

Verwerker / dienst	[IN TE VULLEN]
Onderwerp / duur verwerking	[IN TE VULLEN]
Aard en doel	[IN TE VULLEN]
Gegevens en betrokkenen	[IN TE VULLEN]
Gedocumenteerde instructies	☐ Compleet ☐ Aanpassen
Geheimhouding personeel	☐ Compleet ☐ Aanpassen
Passende beveiliging / TOMs	☐ Compleet ☐ Aanpassen
Subverwerkersprocedure	☐ Compleet ☐ Aanpassen
Datalekmelding / informatie	☐ Compleet ☐ Aanpassen
Hulp bij rechten / DPIA / AP	☐ Compleet ☐ Aanpassen
Verwijdering / teruggave bij einde	☐ Compleet ☐ Aanpassen
Audit / bewijs / medewerking	☐ Compleet ☐ Aanpassen
Doorgifte buiten EER	[IN TE VULLEN / N.v.t.]
Aansprakelijkheid / verzekering	[IN TE VULLEN]
Exit en dataportabiliteit	[IN TE VULLEN]
Afwijkingen / goedkeuring	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F20 | Internationale doorgifte / TIA

Beoordeel opslag, toegang of doorgifte buiten de EER.

Gebruik

Beoordeel ook supporttoegang en subverwerkers; hosting in de EER sluit toegang vanuit derde landen niet automatisch uit.

Verwerking / leverancier / ontvanger	[IN TE VULLEN]
Land(en)	[IN TE VULLEN]
Gegevens / betrokkenen	[IN TE VULLEN]
Privacyrol ontvanger	[IN TE VULLEN]
Doorgiftevorm	☐ Opslag ☐ Support ☐ Remote access ☐ E-mail/document
Mechanisme	☐ Adequaatheid ☐ SCC ☐ BCR ☐ Uitzondering ☐ Anders
Lokale wet-/toegangsrisico's	[IN TE VULLEN]
Encryptie en sleutelcontrole	[IN TE VULLEN]
Pseudonimisering / minimalisatie	[IN TE VULLEN]
Contractuele aanvullende maatregelen	[IN TE VULLEN]
Transparantie / register	[IN TE VULLEN]
Restrisico	☐ Laag ☐ Midden ☐ Hoog
Besluit / voorwaarden	[IN TE VULLEN]
Reviewtrigger / datum	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F21 | Bewaartermijnbesluit

Leg doel, juridische basis, starttrigger, termijn, uitzonderingen en technische verwijdering vast.

Gebruik
Fiscale zevenjaarstermijn geldt niet automatisch voor alle operationele gegevens. Beoordeel per dataset.

Dataset / registercode	[IN TE VULLEN]
Proces / systeem	[IN TE VULLEN]
Doel van bewaring	[IN TE VULLEN]
Wettelijke/contractuele basis	[IN TE VULLEN / geen specifieke plicht]
Starttrigger	☐ Sluiting zaak ☐ Overdracht ☐ Einde contract ☐ Einde dienstverband ☐ Anders
Termijn	[IN TE VULLEN]
Actieve opslag / archief	[IN TE VULLEN]
Back-uprotatie	[IN TE VULLEN]
Legal-holdroute	[IN TE VULLEN]
Automatische verwijdering mogelijk	☐ Ja ☐ Nee, compensatie: [IN TE VULLEN]
Anonimisering mogelijk	[IN TE VULLEN]
Technische test	[IN TE VULLEN]
Juridische/fiscale validatie	[IN TE VULLEN]
Reviewdatum	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F22 | Legal hold

Blokkeer verwijdering gericht en tijdelijk bij claim, onderzoek, klacht, incident of wettelijk bevel.

Gebruik
Een legal hold is niet “alles voor altijd bewaren”. Scope, eigenaar en periodieke review zijn verplicht.

Hold-nummer	[IN TE VULLEN]
Aanleiding / juridische basis	[IN TE VULLEN]
Startdatum / beslisser	[IN TE VULLEN]
Zaak/datasets/personen	[IN TE VULLEN]
Systemen / mailboxen / apparaten	[IN TE VULLEN]
Leveranciers / externe locaties	[IN TE VULLEN]
Bewaarbeheerders geïnformeerd	[IN TE VULLEN]
Automatische verwijdering geblokkeerd	[IN TE VULLEN]
Toegang tot holdmateriaal	[IN TE VULLEN]
Eerste reviewdatum	[IN TE VULLEN]
Periodieke reviews	[IN TE VULLEN]
Opheffingscriterium	[IN TE VULLEN]
Opheffingsdatum / beslisser	[IN TE VULLEN]
Vervolgverwijdering uitgevoerd	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F23 | Verwijdering, anonimisering en vernietiging

Registreer gecontroleerde verwijdering uit bron, afgeleide locaties, apparaten en leveranciers.

Gebruik

Pseudonimisering is geen anonimisering. Verifieer dat heridentificatie redelijkerwijs niet meer mogelijk is.

Opdracht / batchnummer	[IN TE VULLEN]
Dataset / zaken / periode	[IN TE VULLEN]
Bewaartermijn verstreken	☐ Ja ☐ Nee
Legal hold gecontroleerd	☐ Geen ☐ Hold: [IN TE VULLEN]
Bronregistratie	[IN TE VULLEN]
Afgeleide systemen / indexen	[IN TE VULLEN]
Downloads / apparaten / chats	[IN TE VULLEN]
Leveranciers / subverwerkers	[IN TE VULLEN]
Papier / datadragers	[IN TE VULLEN]
Methode	☐ Verwijderen ☐ Anonimiseren ☐ Fysiek vernietigen
Back-uprotatie	[IN TE VULLEN]
Steekproef zoektest	[IN TE VULLEN]
Heridentificatietest indien anoniem	[IN TE VULLEN / N.v.t.]
Afwijkingen / CAPA	[IN TE VULLEN]
Uitvoerder / reviewer / datum	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F24 | GPS-use-case en configuratie

Leg per voertuig, app of dienst het rechtmatige en technisch afgebakende GPS-gebruik vast.

Gebruik

Verboden: heimelijke tracking, onbeperkte personeelscontrole, tracking na dienst zonder uitzondering en brede route-export.

Systeem / voertuigcategorie	[IN TE VULLEN]
Doel(en)	☐ Veiligheid ☐ Dispatch ☐ Check-in ☐ Diefstal ☐ Incident ☐ Bewijs
Betrokkenen	[IN TE VULLEN]
Grondslag / LIA	[IN TE VULLEN]
DPIA-status	[IN TE VULLEN]
OR/PVT/medezeggenschap	[IN TE VULLEN / N.v.t.]
Trackingstart / stop	[IN TE VULLEN]
Privacy mode / privégebruik	[IN TE VULLEN]
Live viewers / rollen	[IN TE VULLEN]
Klantenrapportage	[IN TE VULLEN]
Ruwe retentie	[IN TE VULLEN; uitgangspunt 90 dagen]
Mijlpalen in zaak	[IN TE VULLEN]
Exportbeperking / logging	[IN TE VULLEN]
Privacyinformatie	[IN TE VULLEN]
Test verkeerde zaak / na dienst	[IN TE VULLEN]
Livegangbesluit	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F25 | GPS-, camera- of opname-audit

Controleer doel, configuratie, toegang, raadpleging, retentie, medewerkersinformatie en klachten.

Gebruik

Schort gebruik op wanneer tracking/opname niet meer overeenkomt met het goedgekeurde doel of retentie niet werkt.

Systeem / auditperiode	[IN TE VULLEN]
Doel en LIA/DPIA nog actueel	☐ Ja ☐ Nee
OR/PVT-besluit / informatie	[IN TE VULLEN]
Gebruikers / rollen	[IN TE VULLEN]
Tracking/opname buiten toegestaan venster	[IN TE VULLEN]
Onbevoegde raadpleging / export	[IN TE VULLEN]
Privacymode / uitschakeling getest	[IN TE VULLEN]
Automatische retentie getest	[IN TE VULLEN]
Ruwe data ouder dan termijn	[IN TE VULLEN]
Klantenrapporten minimaal	[IN TE VULLEN]
Klachten / bezwaren	[IN TE VULLEN]
Leverancierswijzigingen	[IN TE VULLEN]
Mogelijk incident	☐ Nee ☐ Ja, nummer: [IN TE VULLEN]
CAPA / opschorting	[IN TE VULLEN]
Volgende audit	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F26 | Beveiligingsincidentmelding

Eerste registratie van cyber-, privacy-, fysiek-, leveranciers- of continuïteitsincident.

Gebruik
Melden vóór volledigheid. De incidentleider vult classificatie en meldbeoordelingen aan.

Incidentnummer	[IN TE VULLEN]
Datum/tijd ontdekking	[IN TE VULLEN]
Datum/tijd kennisname DriveBack	[IN TE VULLEN]
Melder / contact	[IN TE VULLEN]
Locatie / systeem / zaak	[IN TE VULLEN]
Wat is waargenomen	[IN TE VULLEN]
Persoonsgegevens mogelijk geraakt	☐ Nee ☐ Ja ☐ Onbekend
Dienststroom	☐ Mobiliteit ☐ EMS ☐ HR ☐ IT ☐ Leverancier
Beschikbaarheid / integriteit / vertrouwelijkheid	[IN TE VULLEN]
Eerste maatregelen	[IN TE VULLEN]
Bewijs veiliggesteld	[IN TE VULLEN]
Ernst voorlopig	☐ I0 ☐ I1 ☐ I2 ☐ I3 ☐ I4
Incidentleider	[IN TE VULLEN]
Volgende update / beslismoment	[IN TE VULLEN]
Veiligheids-/112-actie	[IN TE VULLEN / N.v.t.]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F27 | Datalekbeoordeling en 72-uursbesluit

Beoordeel of een incident een datalek is, welk risico bestaat en of melding aan de AP en betrokkenen vereist is.

Gebruik
Ook niet-gemelde datalekken komen met motivering in het interne datalekregister.

Incidentnummer	[IN TE VULLEN]
Kennisnametijd / 72-uursdeadline	[IN TE VULLEN]
Aard inbreuk	☐ Vertrouwelijkheid ☐ Integriteit ☐ Beschikbaarheid
Gegevenscategorieën	[IN TE VULLEN]
Bijzondere / ID / GPS / EMS	[IN TE VULLEN]
Aantal / categorie betrokkenen	[IN TE VULLEN]
Ontvanger / dreigingsactor	[IN TE VULLEN]
Versleuteling / toegangsbeveiliging	[IN TE VULLEN]
Toegang / download / verspreiding	[IN TE VULLEN]
Waarschijnlijke gevolgen	[IN TE VULLEN]
Reeds getroffen maatregelen	[IN TE VULLEN]
Risico voor rechten/vrijheden	☐ Onwaarschijnlijk ☐ Risico ☐ Hoog risico
AP-melding	☐ Nee ☐ Ja ☐ Gefaseerd; motivering: [IN TE VULLEN]
Betrokkenen informeren	☐ Nee ☐ Ja; motivering: [IN TE VULLEN]
Andere meldingen	☐ Cbw ☐ Klant ☐ Verzekeraar ☐ Politie ☐ Anders
Besluiter / datum/tijd	[IN TE VULLEN]
AP-meldnummer / vervolg	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F28 | Communicatie aan AP en betrokkenen

Voorbereiding en controle van externe datalekcommunicatie.

Gebruik

Gebruik duidelijke taal en stuur geen massamail met zichtbare adressen. EMS-communicatie krijgt menselijke en waardige review.

Incident / dataleknummer	[IN TE VULLEN]
Doelgroep	☐ AP ☐ Betrokkenen ☐ Opdrachtgever ☐ Verzekeraar ☐ Autoriteit
Feitelijke aard incident	[IN TE VULLEN]
Gegevens en betrokkenen	[IN TE VULLEN]
Waarschijnlijke gevolgen	[IN TE VULLEN]
Getroffen maatregelen	[IN TE VULLEN]
Concrete zelfbescherming	[IN TE VULLEN]
Contactpunt DriveBack	[IN TE VULLEN]
Onzekerheden / gefaseerde update	[IN TE VULLEN]
Juridische/privacyreview	[IN TE VULLEN]
Communicatiereview / waardigheid EMS	[IN TE VULLEN]
Kanaal / ontvangersverificatie	[IN TE VULLEN]
Verzenddatum / bewijs	[IN TE VULLEN]
Reacties / nazorg	[IN TE VULLEN]
Volgende update	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F29 | Bewijsregister en chain of custody

Registreer digitaal of fysiek bewijs bij incident, claim of EMS-kritieke gebeurtenis.

Gebruik
Werk waar mogelijk op een kopie en bescherm het origineel. Elke overdracht is herleidbaar.

Incident / zaak	[IN TE VULLEN]
Bewijs-ID	[IN TE VULLEN]
Omschrijving	[IN TE VULLEN]
Bron / eigenaar	[IN TE VULLEN]
Datum/tijd veiligstelling	[IN TE VULLEN]
Veiliggesteld door	[IN TE VULLEN]
Origineel / kopie	[IN TE VULLEN]
Hash / verificatie	[IN TE VULLEN / N.v.t.]
Opslaglocatie / classificatie	[IN TE VULLEN]
Toegangsbeperking	[IN TE VULLEN]
Overdracht 1: wie/wanneer/waarom	[IN TE VULLEN]
Overdracht 2: wie/wanneer/waarom	[IN TE VULLEN]
Wijzigingen / analyse op kopie	[IN TE VULLEN]
Legal hold / bewaartermijn	[IN TE VULLEN]
Vrijgave / vernietiging	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F30 | Post-incidentreview en CAPA

Leg grondoorzaak, lessen, maatregelen en effectiviteit vast.

Gebruik
Sluit niet op basis van “opgelost”; leg bewijs van implementatie én effectiviteit vast.

Incidentnummer / ernst	[IN TE VULLEN]
Reviewdatum / deelnemers	[IN TE VULLEN]
Feitelijke tijdlijn	[IN TE VULLEN]
Directe oorzaak	[IN TE VULLEN]
Achterliggende oorzaken mens/proces/techniek	[IN TE VULLEN]
Gemiste preventie/detectie	[IN TE VULLEN]
Wat werkte goed	[IN TE VULLEN]
Herstelmaatregel	[IN TE VULLEN]
Preventieve maatregel	[IN TE VULLEN]
Detectie-/responsverbetering	[IN TE VULLEN]
Eigenaren en deadlines	[IN TE VULLEN]
Training / beleid / contract aanpassen	[IN TE VULLEN]
Effectiviteitstest	[IN TE VULLEN]
Restrisico	[IN TE VULLEN]
Sluitingsbesluit	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F31 | Back-up- en hersteltest

Test beschikbaarheid, integriteit, toegangsrechten en operationele bruikbaarheid van herstel.

Gebruik
Een back-upjob zonder aantoonbaar herstel is onvoldoende. Test ook rechten en dossierintegriteit.

Testdatum / scenario	[IN TE VULLEN]
Systeem / dataset	[IN TE VULLEN]
Classificatie / kritikaliteit	[IN TE VULLEN]
Doel-RPO / doel-RTO	[IN TE VULLEN]
Geselecteerde back-up / datum	[IN TE VULLEN]
Back-up gescheiden / versleuteld	[IN TE VULLEN]
Herstelomgeving	[IN TE VULLEN]
Werkelijk gegevensverlies (RPO)	[IN TE VULLEN]
Werkelijke hersteltijd (RTO)	[IN TE VULLEN]
Integriteit / volledigheid	[IN TE VULLEN]
Autorisaties / logging na herstel	[IN TE VULLEN]
Applicatie/zaak bruikbaar	[IN TE VULLEN]
Fallback en reconciliatie getest	[IN TE VULLEN]
Afwijkingen / CAPA	[IN TE VULLEN]
Conclusie	☐ Geslaagd ☐ Voorwaardelijk ☐ Mislukt

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F32 | Interne audit en steekproef

Plan en rapporteer privacy- of beveiligingsaudit.

Gebruik

Audit minimaal toegang, retentie, leveranciers, datalekrespons, GPS en EMS-custody op een risicogebaseerde cyclus.

Auditcode / periode	[IN TE VULLEN]
Scope / norm / criteria	[IN TE VULLEN]
Auditor(s) / onafhankelijkheid	[IN TE VULLEN]
Processen / systemen	[IN TE VULLEN]
Steekproefomvang	[IN TE VULLEN]
Bewijs / interviews / exports	[IN TE VULLEN]
Positieve bevindingen	[IN TE VULLEN]
Observaties	[IN TE VULLEN]
Minor afwijkingen	[IN TE VULLEN]
Major afwijkingen	[IN TE VULLEN]
Kritieke afwijkingen	[IN TE VULLEN]
Mogelijke incidenten	[IN TE VULLEN]
Actieplan / eigenaren / deadlines	[IN TE VULLEN]
Verificatie effectiviteit	[IN TE VULLEN]
Rapportage directie	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F33 | KPI/KRI en managementreview

Gebruik voor kwartaal- of jaarreview van privacy- en informatiebeveiliging.

Gebruik
Besluiten zijn concreet en worden gevolgd tot aantoonbare afronding.

Reviewperiode / datum	[IN TE VULLEN]
Deelnemers	[IN TE VULLEN]
Open acties vorige review	[IN TE VULLEN]
Incidenten / datalekken / trends	[IN TE VULLEN]
KPI/KRI afwijkingen	[IN TE VULLEN]
Audits / bevindingen	[IN TE VULLEN]
Toegang / retentie / GPS	[IN TE VULLEN]
Back-up / continuïteit	[IN TE VULLEN]
Leveranciers / subverwerkers	[IN TE VULLEN]
Privacyverzoeken / klachten	[IN TE VULLEN]
Wetswijzigingen / Cbw-toets	[IN TE VULLEN]
Middelen / budget / capaciteit	[IN TE VULLEN]
Risicoacceptaties	[IN TE VULLEN]
Besluiten / eigenaren / deadlines	[IN TE VULLEN]
Volgende review	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F34 | EMS privacy-, identiteit- en custody-incident

Gebruik bij identiteitstwijfel, documentconflict, sealbreuk, custodygat, ongepaste fotografie of onbevoegde overdracht.

Gebruik

Automatisch I4. Geen opening, resealing, correctie of verdere overdracht zonder bevoegde schriftelijke beslissing.

EMS-zaak / incidentnummer	[IN TE VULLEN]
Datum/tijd / locatie	[IN TE VULLEN]
Melding door	[IN TE VULLEN]
Type	☐ Identiteit ☐ Document ☐ Seal ☐ Custody ☐ Overdracht ☐ Beeld ☐ Bezitting
Transport/overdracht op HOLD	☐ Ja ☐ Nee, motivering: [IN TE VULLEN]
Waardige/veilige fysieke situatie	[IN TE VULLEN]
Identificatoren en afwijking	[IN TE VULLEN]
Documenten / bronpartijen	[IN TE VULLEN]
Seal / kist / conditie	[IN TE VULLEN]
Custodytijdlijn	[IN TE VULLEN]
Vierogencontrole	[IN TE VULLEN]
Gegevens / levende betrokkenen geraakt	[IN TE VULLEN]
Autoriteiten / opdrachtgever / verzekeraar	[IN TE VULLEN]
AP-/datalekbeoordeling	[IN TE VULLEN]
Herstartvrijgave en voorwaarden	[IN TE VULLEN]
Nabestaandencommunicatie / nazorg	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F35 | Opleiding, geheimhouding en autorisatie

Bewijs dat een medewerker of ingehuurde kracht vóór toegang en periodiek is geïnstrueerd en beoordeeld.

Gebruik
Kritieke toegang wordt niet geactiveerd voordat training, geheimhouding, MFA en functiegoedkeuring compleet zijn.

Naam / functie / organisatie	[IN TE VULLEN]
Rol(len)	[IN TE VULLEN]
Geheimhouding getekend	[IN TE VULLEN]
Basistraining privacy/security	[IN TE VULLEN]
Phishing/datalekscenario	[IN TE VULLEN]
Dossierbeheer / veilige communicatie	[IN TE VULLEN]
GPS/monitoringmodule	[IN TE VULLEN / N.v.t.]
EMS-privacy/waardigheid/custody	[IN TE VULLEN / N.v.t.]
HR-/beheer-/incidentmodule	[IN TE VULLEN / N.v.t.]
Toetsresultaat	[IN TE VULLEN]
Praktijkbeoordeling	[IN TE VULLEN]
Autorisatie	☐ Volledig ☐ Beperkt ☐ Niet verleend
Beperkingen	[IN TE VULLEN]
Geldig tot / hertraining	[IN TE VULLEN]
Ontvangst dossier / instructies	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

DB-PIB-F36 | Jaarlijkse privacy- en beveiligingsauditkalender

Plan vaste beheersactiviteiten en bewijs over het kalenderjaar.

Gebruik

Pas de kalender aan risico en groei aan. Ernstige incidenten of wijzigingen activeren tussentijdse audits.

Kalenderjaar	[IN TE VULLEN]
Q1: toegang / leveranciers / Cbw-toets	[IN TE VULLEN]
Q1: back-upherstel / datalekoefening	[IN TE VULLEN]
Q2: verwerkingsregister / privacyverklaringen	[IN TE VULLEN]
Q2: GPS/camera/opname-audit	[IN TE VULLEN]
Q2: EMS-custodydossiers steekproef	[IN TE VULLEN]
Q3: DPIA/LIA-review / internationale doorgifte	[IN TE VULLEN]
Q3: ransomware- en continuïteitsoefening	[IN TE VULLEN]
Q3: autorisaties / JML	[IN TE VULLEN]
Q4: retentie/verwijdering / legal holds	[IN TE VULLEN]
Q4: managementreview / begroting	[IN TE VULLEN]
Jaarlijks: training / phishingtest	[IN TE VULLEN]
Maandelijks: KPI/KRI / open P0	[IN TE VULLEN]
Kwartaal: kritieke leveranciers / hersteltest	[IN TE VULLEN]
Eigenaren / vervangers	[IN TE VULLEN]
Wijzigingen / goedkeuring	[IN TE VULLEN]

Opgesteld door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Gecontroleerd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Goedgekeurd door	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

Bijlage A | Initiële verwerkingsinventaris DriveBack & EMS

Onderstaande inventaris vormt de inhoudelijke startset voor het centrale register. Iedere regel moet vóór livegang worden aangevuld met systemen, concrete ontvangers, beveiliging, verantwoordelijke en definitieve juridische validatie.

Code	Verwerking	Betrokkenen	Gegevens	Grondslag / basis	Uitgangstermijn
DB-VR-001	Website/ contactaanvragen	Prospects/klanten	Contact, aanvraag, IP/logs	Precontract / gerechtvaardigd belang	6 maanden na afhandeling
DB-VR-002	B2B-relatiebeheer	Contactpersonen opdrachtgevers/partners	Zakelijk contact, functie, communicatie	Gerechtvaardigd belang / overeenkomst	Tot 2 jaar na einde relatie; fiscale stukken apart
DB-VR-003	24/7 mobiliteitsintake	Melder, bestuurder, eigenaar, passagiers	ID/contact, locatie, voertuig, uitval, communicatie	Overeenkomst / vitaal belang / gerechtvaardigd belang	Kernzaak 2 jaar
DB-VR-004	Mobiliteitsplanning en dispatch	Bestuurder, chauffeur, partners	Reis, route, locatie, opdracht, contact	Overeenkomst / gerechtvaardigd belang	Kernzaak 2 jaar; tijdelijke reisdata kort
DB-VR-005	GPS en check-ins	Chauffeurs, bestuurders	Live locatie, route, tijd, voertuig	Gerechtvaardigd belang na LIA/DPIA	Ruw 90 dagen; mijlpalen 2 jaar
DB-VR-006	Voertuiginspectie en overdracht	Eigenaar/bestuurder/ ontvanger	Voertuig, kenteken, foto's, handtekening	Overeenkomst / bewijs	2 jaar; claimset legal hold
DB-VR-007	Reis- en hotelboekingen	Medewerkers, chauffeurs, klanten	Naam, contact, ticket, ID indien vereist	Overeenkomst	Na doelbereik; fiscale boeking apart
DB-VR-008	B2B-portaal en rapportage	Opdrachtgevercontact, verzekerde/bestuurder	Zaakstatus, kosten, minimale bewijsdata	Overeenkomst / rolafhankelijk	Volgens contract en zaaktermijn
DB-VR-009	Klachten en claims	Klant, betrokkene, medewerker, partner	Dossier, communicatie, schade, bewijs	Overeenkomst / gerechtvaardigd belang / wet	3-5 jaar of legal hold
DB-VR-010	EMS-intake en opdracht	Opdrachtgever, nabestaanden, professionals	Contact, opdracht, transport, documenten	Overeenkomst / gerechtvaardigd belang; levende betrokkenen	EMS-kern 2 jaar, daarna review
DB-VR-011	EMS-document- en custodyketen	Nabestaanden/ professionals/crew	Identificatoren, vrijgave, seal, custody, overdracht	Overeenkomst / wettelijke/documentaire noodzaak	2 jaar, daarna juridische review/legal hold
DB-VR-012	EMS-veiligheidsinformatie	EMS-crew, betrokken professionals	Functionele infectie-/blootstellingsinfo	Veiligheid + toepasselijke bijzondere-gegevensuitzondering	Zo kort mogelijk; kerninstructie volgens zaak
DB-VR-013	Buitenlandse partnercoördinatie	Contactpersonen, nabestaanden/opdrachtgever	Contact, transportdocumenten, minimale persoonsgegevens	Overeenkomst / gerechtvaardigd belang / doorgiftebasis	Zaaktermijn; tijdelijke kopieën kort
DB-VR-014	Facturatie en administratie	Klanten, leveranciers, medewerkers	Naam, adres, bank, factuur, kosten	Overeenkomst / fiscale wet	Fiscale basisadministratie 7 jaar
DB-VR-015	Personeelsadministratie	Medewerkers	ID, contract, loon, functie, opleiding, verlof	Overeenkomst / wet	Categorieafhankelijk; algemeen 2 jaar na einde
DB-VR-016	Verzuim en re-integratie	Medewerkers	Ziekmelding, functionele inzetbaarheid, afspraken	Arbeidsrecht / wettelijke verplichting	Volgens verzuim- en arbeidsrechtelijke termijn
DB-VR-017	Werving en selectie	Sollicitanten	Contact, cv, brief, beoordeling, VOG-status	Precontract / gerechtvaardigd belang / toestemming talentpool	4 weken; 1 jaar met toestemming
DB-VR-018	Account- en toegangsbeheer	Medewerkers/externen	Identiteit, rol, account, logs, apparaat	Gerechtvaardigd belang / overeenkomst	Accountduur + review; logs 12/24 maanden
DB-VR-019	Beveiligingslogging en monitoring	Gebruikers/externen	Login, MFA, acties, IP, device, exports	Gerechtvaardigd belang na beoordeling	12 maanden; beheerlogs 24 maanden
DB-VR-020	Gespreksopnamen / kwaliteitscontrole	Bellers, medewerkers	Audio, nummer, tijd, zaakreferentie	Gerechtvaardigd belang na LIA/DPIA	Uitgangspunt 90 dagen
DB-VR-021	Camera/dashcam	Medewerkers, weggebruikers, bezoekers	Beeld, voertuig, tijd/locatie	Gerechtvaardigd belang na LIA/DPIA	Max. 28 dagen tenzij incident

Code	Verwerking	Betrokkenen	Gegevens	Grondslag / basis	Uitgangstermijn
DB-VR-022	Incidenten en datalekken	Betrokkenen, medewerkers, ontvangers	Incident, logs, communicatie, risico, bewijs	Wettelijke verplichting / gerechtvaardigd belang	Incident-/ datalekregister 5 jaar intern
DB-VR-023	Rechten en privacyklachten	Verzoekers/klagers	Identiteit, verzoek, zoekresultaat, besluit	Wettelijke verplichting	3 jaar na afsluiting
DB-VR-024	Leveranciers- en verwerkersbeheer	Contactpersonen/ externen	Contact, contract, accounts, assurance	Overeenkomst / gerechtvaardigd belang	7 jaar na einde contract voor kernbewijs
DB-VR-025	Training en autorisatie	Medewerkers/externen	Deelname, toets, autorisatie, geldigheid	Overeenkomst / gerechtvaardigd belang / wet	Dienstverband + relevante bewijsperiode

Bijlage B | Initiële privacy- en beveiligingsrisicoanalyse

Dit register bevat de voor DriveBack meest waarschijnlijke startscenario's. Kans, impact, bestaande beheersing, restrisico en eigenaar worden vóór livegang per systeem en proces gekwantificeerd.

ID	Scenario	Inherent	Belangrijkste maatregelen	Eigenaar
R-01	Verkeerde e-mail/zaakbijlage	Hoog	Ontvangercheck, veilige link, QC-02, DLP waar mogelijk	Meldkamer/IT
R-02	Phishing/ accountovername	Kritiek	MFA, filters, training, token/sessierespons	IT/security
R-03	Ransomware en uitval meldkamer	Kritiek	Segmentatie, EDR, back-ups, fallback, oefening	Directie/IT
R-04	Onbevoegde EMS-inzage	Kritiek	Aparte rollen, zaaktoewijzing, logging, audit	EMS/IT/privacy
R-05	GPS buiten dienst / doelverschuiving	Hoog	LIA/DPIA, privacy mode, 90-dagenretentie, audit	Planning/privacy
R-06	Verloren telefoon/laptop	Hoog	MDM, encryptie, remote wipe, minimale offline data	IT/gebruiker
R-07	Onvolledige custody / misidentificatie EMS	Kritiek	Vierogen, seal/documentcheck, I4-HOLD	EMS-leiding
R-08	Leveranciersdatalek / subverwerker	Hoog	Due diligence, DPA, meldtermijn, exit, monitoring	Inkoop/privacy/IT
R-09	Ongeteste back-up	Kritiek	Kwartaal hersteltest, RPO/RTO, gescheiden kopie	IT/continuïteit
R-10	Shadow IT / privé-WhatsApp	Hoog	Zakelijke apps, MDM, training, dossiermigratie, audit	Leiding/IT
R-11	Te lange retentie ID/GPS/opnamen	Hoog	Automatische retentie, matrix, maandcontrole	Privacy/systeemeigenaar
R-12	Brede portaal- of groepsrechten	Hoog	RBAC, JML, toegangsreview, negatieve test	IT/informatie-eigenaar
R-13	Buitenlandse doorgifte zonder basis	Hoog	Partnerregister, TIA/SCC, minimale set, verificatie	Privacy/operations
R-14	Ongepaste EMS-fotografie/publicatie	Kritiek	Verbod, zakelijke camera, directe upload, QC-10	EMS/HR/privacy
R-15	Medische details in vrije tekst	Hoog	Functionele velden, training, beperkte toegang, opschoning	Operations/HR
R-16	Beheeraccountmisbruik	Kritiek	Separate admin, JIT, break-glass, sessielog/review	IT/directie
R-17	Business e-mail compromise/betalingsfraude	Kritiek	Vierogen, tweede kanaal, bankwijzigingscontrole	Financiën/directie
R-18	Onvoldoende 72-uursdatalekrespons	Hoog	24/7 route, formulieren, oefening, mandaten	Privacy/directie
R-19	Papierdossier verloren in voertuig/hotel	Hoog	Minimale print, gesloten tas, custody, vernietiging	Operations
R-20	AI-tool ontvangt vertrouwelijke data	Hoog	AI-register, blokkade publieke tools, contract/configuratie	IT/privacy

Bijlage C | Contact-, mandaat- en escalatieregister

De geel gemarkeerde velden moeten vóór formele invoering zijn ingevuld en 24/7 getest. Externe nummers en portals worden in het beveiligde register onderhouden, niet uitsluitend in een papieren afdruk.

Rol / partij	Naam	24/7 contact	Mandaat / taak
Directie / eindverantwoordelijke	[IN TE VULLEN]	[IN TE VULLEN]	Risicoacceptatie, externe meldingen, crisisbesluit
Incidentleider primair	[IN TE VULLEN]	[IN TE VULLEN]	I2-I4 leiding, containment, tijdlijn
Incidentleider vervanger	[IN TE VULLEN]	[IN TE VULLEN]	Vervanging 24/7
Privacycoördinator / FG	[IN TE VULLEN]	[IN TE VULLEN]	AVG-beoordeling, AP, rechten, DPIA
IT/security primair	[IN TE VULLEN]	[IN TE VULLEN]	Accounts, isolatie, logs, herstel
IT/security vervanger	[IN TE VULLEN]	[IN TE VULLEN]	24/7 technische vervanging
Meldkamer/planning leiding	[IN TE VULLEN]	[IN TE VULLEN]	Fallback, operatie, klantstatus
EMS-leiding	[IN TE VULLEN]	[IN TE VULLEN]	I4 identiteit/custody/waardigheid
HR/arbodienst	[IN TE VULLEN]	[IN TE VULLEN]	Personeelsprivacy, blootstelling, nazorg
Communicatie/woordvoering	[IN TE VULLEN]	[IN TE VULLEN]	Betrokkenen, klanten, media
Juridisch / ARAG of adviseur	[IN TE VULLEN]	[IN TE VULLEN]	Juridische toets, claims, autoriteiten
Cyberverzekering / verzekeraar	[IN TE VULLEN]	[IN TE VULLEN]	Polismelding en responseondersteuning
AFAS / kernleverancier	[IN TE VULLEN]	[IN TE VULLEN]	Storingen, datalek, herstel
Telefonie / meldkamerleverancier	[IN TE VULLEN]	[IN TE VULLEN]	Uitval, opnamen, incident
GPS/telematicaleverancier	[IN TE VULLEN]	[IN TE VULLEN]	Trackinguitval, datalek, export

Bijlage D | Implementatiematrix vóór formele livegang

Prio	Domein	Acceptatiecriterium	Eigenaar	Deadline	Status
P0	Governance	Directie, privacy, IT, incidentleider en vervangers benoemd	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	Incidentrespons	24/7 nummer, ernstmatrix, 72-uursbesluit en oefening getest	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	Autorisaties	Rollenmatrix technisch geïmplementeerd en negatief getest	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	MFA	MFA op e-mail, cloud, dossier, VPN, beheer en GPS-portaal	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	EMS-scheiding	Aparte rollen, custody, vierogen en beeldbeperking actief	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	Back-up	Gescheiden back-up en herstel/fallback aantoonbaar getest	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	Leveranciers	DPA's en incidentcontacten voor kritieke leveranciers gereed	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	GPS	LIA/DPIA, informatie, medezeggenschap, privacy mode en retentie gereed	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	Retentie	Automatische verwijdering voor ID, GPS, opnamen en camera getest	[IN TE VULLEN]	[IN TE VULLEN]	Open
P0	Bronregistratie	AFAS/centrale omgeving, zaakcodes en tijdelijke kanalen geregeld	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	FG-toets	Formele FG-noodzaakstoets en benoeming/privacycontact	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Cbw-toets	Toepasselijkheid Cyberbeveiligingswet vóór 15-08-2026 vastgesteld	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Register	Verwerkingsregister en dataflows gevalideerd	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Privacyinformatie	Website, klant, GPS, personeel en EMS gepubliceerd	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Rechten	Verzoekprocedure en zoek-/redactietest uitgevoerd	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Assetbeheer	Asset-, systeem-, koppelingen- en leveranciersregister compleet	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Training	Alle kritieke rollen getraind en getoetst	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Audits	Jaarplanning, KPI/KRI en managementreview vastgesteld	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	Internationale doorgifte	Buitenlandse partners en supportlanden beoordeeld	[IN TE VULLEN]	[IN TE VULLEN]	Open
P1	AI/BYOD	Gebruik formeel toegestaan, beperkt of verboden en technisch ondersteund	[IN TE VULLEN]	[IN TE VULLEN]	Open

Bijlage E | Juridisch en normatief bronnenregister

Bronnen zijn gecontroleerd op 5 augustus 2026. DriveBack gebruikt officiële bronnen als uitgangspunt en beoordeelt actualiteit minimaal per kwartaal en vóór materiële beleidswijziging.

Bron	Uitgever	Vindplaats	Gebruik in dossier
Algemene verordening gegevensbescherming (EU) 2016/679	EUR-Lex	https://eur-lex.europa.eu/eli/reg/2016/679/oj	AVG-grondslag, beginselen, rechten, beveiliging, datalekken
Uitvoeringswet AVG	Overheid.nl	https://wetten.overheid.nl/BWBR0040940/	Nederlandse uitvoering en uitzonderingen
Verantwoordingsplicht / verwerkingsregister	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verantwoordingsplicht	Register, bewijs en accountability
Grondslagen AVG	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/grondslagen-avg-uitgelegd	Zes grondslagen
DPIA	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia	Hoog privacyrisico en DPIA
Datalek: wat te doen	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen	72 uur, betrokkenen, intern register
Datalek melden	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/zo-meldt-u-een-datalek	Meldproces en termijn
Verwerkersovereenkomst	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/verwerkersovereenkomst	Artikel 28-afspraken
Controle werknemers	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/controle-van-werknemers	Voorwaarden monitoring
OR en personeelsvolgsystemen	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/ondernemingsraad/de-or-en-personeelsvolgsystemen	Instemmingsrecht personeelsvolgsystemen
Persoonsgegevens en overledenen	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens	AVG geldt voor levende natuurlijke personen
Doorgifte buiten de EER	Autoriteit Persoonsgegevens	https://www.autoriteitpersoonsgegevens.nl/themas/internationaal/doorgifte-binnen-en-buiten-de-eer/doorgifte-persoonsgegevens-buiten-de-eer	Doorgiftemechanismen
Cyberbeveiligingswet (NIS2)	NCSC	https://www.ncsc.nl/cyberbeveiligingswet-nis2	Inwerkingtreding 15 augustus 2026 en verplichtingen
Veelgestelde vragen Cyberbeveiligingswet	NCSC	https://www.ncsc.nl/cyberbeveiligingswet-nis2/faq-cyberbeveiligingswet-nis2	Scope, sector en omvang
ISO/IEC 27001:2022	ISO	https://www.iso.org/standard/27001	ISMS en vertrouwelijkheid, integriteit, beschikbaarheid
Arbeidsomstandigheden en werkgeverschap	Arboportaal / Rijksoverheid	https://www.arboportaal.nl/	Veiligheid, gezondheid, arbodienst

Actualiteitsbeheer

De Cyberbeveiligingswet treedt volgens het NCSC op 15 augustus 2026 in werking. Dit dossier is uitgegeven op 5 augustus 2026. DriveBack moet de toepasselijkheid en definitieve uitvoeringsregels onmiddellijk vóór en na die datum opnieuw controleren en de uitkomst bestuurlijk vastleggen.

Ontvangst, invoering en jaarlijkse herbevestiging

Ondertekening bevestigt ontvangst en kennisname. Zij vervangt niet de vereiste opleiding, technische implementatie, juridische toets of daadwerkelijke naleving.

Werkgever / directie	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Documenteigenaar	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Privacyverantwoordelijke	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Informatiebeveiligingsverantwoordelijke	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]
Medezeggenschap indien van toepassing	[IN TE VULLEN]	**Datum**	[IN TE VULLEN]

Formele ingebruikname

Voor bindende invoering worden ten minste de P0-punten uit Bijlage D gesloten, de open [IN TE VULLEN]-velden bekrachtigd, medewerkers geïnstrueerd, systemen getest en relevante contracten ondertekend. Het dossier wordt daarna gepubliceerd met een concrete ingangsdatum en vervangt eerdere tegenstrijdige instructies.

Einde document - DB-PIB-001 | Versie 1.0 | Uitgiftedatum 5 augustus 2026

Aanvulling – HIPAA, PHI en websitebeveiliging

Documentcode: DB-PIB-001 | Aanvulling bij versie 1.1 | Registratiedatum: 18 oktober 2026 | Opgegeven ingangsdatum: 1 oktober 2026 (met terugwerkende kracht).

1. Reikwijdte en status van HIPAA

DriveBack streeft naar informatiebeveiliging volgens de actueel toepasselijke eisen van de AVG en, uitsluitend waar de Amerikaanse HIPAA-wetgeving daadwerkelijk van toepassing is, de relevante HIPAA Privacy Rule, Security Rule en Breach Notification Rule. De uitspraak dat DriveBack volledig HIPAA-conform is of aan de strengste nieuwste HIPAA-eisen voldoet, is zonder vastgelegde toepasselijkheidstoets, technische verificatie, contractuele onderbouwing en controleerbare auditbevindingen niet vastgesteld. Deze aanvulling is geen HIPAA-certificaat of complianceverklaring.

2. PHI-beveiliging op de website

De organisatie meldt dat op de website een beveiligingsmaatregel voor PHI (Protected Health Information) is geactiveerd. De technische configuratie, reikwijdte en werking daarvan zijn ten tijde van deze documentwijziging niet onafhankelijk geverifieerd. Het enkele activeren van een beveiligingsfunctie maakt de website niet automatisch geschikt voor het verzamelen, verwerken of opslaan van gezondheidsgegevens of PHI. Tot verificatie worden gezondheidsgegevens via publieke webformulieren niet opgevraagd.

3. Vereiste technische en organisatorische toets

- Inventariseer of de website, formulieren, hosting, e-mail en externe diensten daadwerkelijk PHI verwerken en of HIPAA juridisch van toepassing is.
- Documenteer de exacte Wix-/website-instellingen, de verwerkers en subverwerkers, opslaglocaties en internationale doorgiften.
- Controleer toegangsrechten, MFA, versleuteling tijdens transport en opslag, auditlogs, bewaartermijnen, back-ups, incidentrespons en veilige verwijdering.
- Controleer of wettelijk noodzakelijke contracten, waaronder eventuele Business Associate Agreements, zijn afgesloten waar HIPAA dat vereist.
- Laat de maatregelen testen en formeel accorderen, met bewijsstukken, door de aangewezen privacy- en informatiebeveiligingsverantwoordelijke.

4. Verantwoordelijkheid en opvolging

Verantwoordelijke voor registratie en besluitvorming: J.B. Verdonk. Gewenste beleidsingangsdatum: 01-10-2026, met terugwerkende kracht administratief vastgelegd. Dit legt geen onbewezen technische werking of historische ondertekening vast. Bevestiging van HIPAA-naleving en PHI-beveiliging volgt uitsluitend op basis van toetsbare bewijsstukken.