Handreiking Beveiligingsmaatregelen

SURF Juridisch Normenkader (Cloud)services, bijlage C

Utrecht, 20-04-2018
Versienummer: 3.0

Colofon

Handreiking Beveiligingsmaatregelen
SURF SURF Juridisch Normenkader (Cloud)services, bijlage C Normenkader (Cloud)services, Bijlage C

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inleiding

Op 13 november 2013 heeft SURF het *SURF Juridisch Normenkader (Cloud)services* gepubliceerd en in februari 2016 aangepast aan nieuwe wet- en regelgeving en naar aanleiding van het gebruik gedurende de afgelopen twee jaar. De Model Verwerkersovereenkomst verplicht de leverancier om passende maatregelen te treffen voor de fysieke en logische beveiliging van de geleverde dienst.
De set maatregelen in deze tekst is bedoeld als handreiking om het begrip “passende beveiligingsmaatregelen” concreet te maken. Het is geen voorschrift, het is mogelijk om met andere maatregelen hetzelfde of een beter effect te bereiken.

De gesuggereerde maatregelen zijn ingedeeld in de volgende categorieën:

1. Beleid en organisatie.
2. Toegangsbeveiliging.
3. Beheer van technische kwetsbaarheden en anti-malware.
4. Vertrouwelijkheid en integriteit van gegevens en Privacy.
5. Controle en logging.

Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) stelt met betrekking tot beveiliging het volgende:

“Rekening houdend met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:

a) de pseudonimisering en versleuteling van persoonsgegevens;
b) het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) *een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.”*[1]

Het CBP (nu de Autoriteit Persoonsgegevens) stelt dat ‘*de maatregelen zijn gebaseerd op een risicoanalyse en dekken de risico’s zodanig af dat aan de betrouwbaarheid wordt voldaan. Naarmate de vereiste betrouwbaarheid c.q. het vereiste beveiligingsniveau hoger is, treft de verantwoordelijke meer en zwaardere beveiligingsmaatregelen om de aanwezige risico’s af te dekken en het vereiste beveiligingsniveau daadwerkelijk te garanderen.*[2] Ook een verwerker dient volgens de AVG deze maatregelen te treffen. Deze handreiking bevat een aantal maatregelen waaraan de beveiliging bij de verwerking van persoonsgegevens dient te voldoen – afhankelijk van de risicoklasse.

De maatregelen zijn opgebouwd rond paragraaf 3.2 van het CBP richtsnoer " *Beveiliging van Persoonsgegevens* " d.d. februari 2013[3] van de Autoriteit Persoonsgegevens. Ook het richtsnoer gaat uit

[1] Artikel 32 AVG.
[2] CBP Richtsnoer “*Beveiliging van Persoonsgegevens*” § 2.4
[3] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf (geconsulteerd op 19/04/2016)

van een risicoanalyse om een goed afgewogen keuze te maken voor de te nemen beveiligingsmaatregelen. Het verdient aanbeveling om een risicoanalyse te maken en regelmatig te evalueren.

Paragraaf 3.2 van het CBP richtsnoer " *Beveiliging van Persoonsgegevens*" verwijst veelvuldig naar ISO 27002:2007, de praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging. Er wordt echter niet naar alle categorieën van maatregelen verwezen. Daarom bevatten de tabellen op de volgende pagina's een selectie van maatregelen en ontbreken bijvoorbeeld maatregelen die betrekking hebben op de betrouwbaarheid van personeel, terwijl hier, afhankelijk van de risicocategorie, ook maatregelen gewenst zijn. In de paragraaf "Relevante standaarden/documenten" wordt verwezen naar standaarden, waarin de leverancier aanvullende informatie kan vinden.

Toegevoegd ten opzichte van paragraaf 3.2 uit het bovengenoemd CBP richtsnoer zijn de maatregelen rond wijzigingsbeheer. Wijzigingsbeheer is dermate wezenlijk voor de beschikbaarheid, integriteit en vertrouwelijkheid van gegevensverwerking dat het aan de set is toegevoegd.

Beschikbaarheid van informatiesystemen valt buiten de reikwijdte van de set maatregelen in deze handreiking. Het Juridisch Normenkader veronderstelt dat in de Overeenkomst of in een Service Level Overeenkomst criteria voor de beschikbaarheid overeen worden gekomen.

Specifieke maatregelen rondom applicatiecontroles zijn niet opgenomen, omdat de benodigde applicatiecontroles sterk bepaald worden door het type toepassing dat de dienst vormt. Aangeraden wordt de vereiste applicatiecontroles op te nemen in een set waarin de functionele vereisten zijn beschreven. Bij het ontwikkelen en testen van Web applicaties is de OWASP[4] Top Tien een krachtig hulpmiddel. De OWASP Top Tien *Most Critical Web Application Security Risks*[5] geeft aan welke tien beveiligingsproblemen voor web applicaties het meest voorkomen. De OWASP Top 10 *Proactive Controls*[6] geeft web applicatieontwikkelaars een lijst technieken die in ieder applicatie-ontwikkelproject toegepast zouden moeten worden.

Passende beveiligingsmaatregelen

De maatregelentabel bevat de maatregelen die passend zijn bij verwerkingen van risicoklassen Laag (publiek niveau) en Midden zoals in het Juridisch Normenkader gedefinieerd. Maatregelen die alleen van toepassing zijn op risicoklasse Hoog zijn rood gemarkeerd en hebben de aanduiding "HOOG" in de eerste kolom. Deze maatregelen, in combinatie met de basismaatregelen, worden passend geacht bij de verwerkingen van bijzondere persoonsgegevens (zoals gedefinieerd in artikel 9 van de AVG) en indien de verwerking om andere redenen – bijvoorbeeld de omvang van de verwerking– toch als zeer risicovol moet worden aangemerkt.

Relevante standaarden/documenten

Naast het CBP richtsnoer "*Beveiliging van Persoonsgegevens*" zijn een aantal standaarden en documenten geraadpleegd voor deze handreiking:

- NEN-ISO/IEC 27001:2013 – Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging – Eisen.

[4] Het Open Web Application Security Project (OWASP) is een open source-project rond computerbeveiliging. Individuen, scholen en bedrijven delen via dit platform informatie en technieken. Zie: https://www.owasp.org

[5] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[6] https://www.owasp.org/index.php/OWASP_Proactive_Controls

- NEN-ISO/IEC 27002:2013 – Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging.
- NEN-ISO/IEC 27005:2011 – Information technology — Security techniques — Information security risk management.
- NEN-ISO/IEC 27017:2015 – Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- NEN-ISO/IEC 27018:2014 – Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
- NEN-ISO/IEC 27033-1:2015 – Information technology - Security techniques - Network security - Part 1: Overview and concepts.
- NEN-ISO/IEC 27035-1:2016 – Information technology - Security techniques - Information security incident management – Part 2: Guidelines to plan and prepare for incident response.
- NIST SP800-12r1 (2017) – Introduction to Computer Security — "The NIST Handbook".
- NIST SP800-30r1 (2012) – Guide for Conducting Risk Assessments.
- NIST SP 800-53r4 (2013/15) – Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP800-61r2 (2012) – Computer Security Incident Handling Guide.
- Autoriteit Persoonsgegevens - Beleidsregels voor toepassing van artikel 34a van de Wbp.[7]
- ENISA – Algorithms, key size and parameters report – 2014.[8]
- Common Criteria – Certified Products.[9]
- PCI Data Security Standard – v3.2.[10]
- CIS Critical Security Controls for Effective Cyber Defense.[11]

[7] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/thematische-beleidsregels/beleidsregels-meldplicht-datalekken-2015 (geconsulteerd op 11/04/2018)

[8] https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014 (geconsulteerd op 11/04/2018)

[9] https://www.commoncriteriaportal.org/products/ (geconsulteerd op 11/04/2018)

[10] https://www.pcisecuritystandards.org/ (geconsulteerd op 20/04/2016)

[11] https://www.cisecurity.org/critical-controls.cfm (geconsulteerd op 11/04/2018)

Tabel met beveiligingsmaatregelen

1 Beleid en organisatie

Een door de directie vastgesteld en uitgedragen beveiligingsbeleid is de basis van alle informatiebeveiliging. Het beleid wordt gebaseerd op een analyse van de risico's. Personeel, zowel vaste en tijdelijke werknemers als ingehuurd personeel, is zich bewust van het beleid en kent zijn verantwoordelijkheden. Voor het beheer van incidenten, inclusief datalekken, wijzigingen en beschikbaarheid is een proces ingericht.

#	Maatregel	Referentie
	Actueel informatiebeveiligingsbeleid en organisatie van informatiebeveiliging	
1.1	De directie van de leverancier heeft een Informatiebeveiligingsbeleid vastgesteld en communiceert dit aantoonbaar op regelmatige basis (jaarlijks), zowel intern als aan relevante externe partijen.	ISO 27002:2013 §5.1.1
1.2	Het informatiebeveiligingsbeleid wordt tenminste jaarlijks beoordeeld of als zich een grote verandering heeft voorgedaan.	ISO 27002:2013 §5.1.2
1.3	De leverancier heeft de verantwoordelijkheden met betrekking tot Informatiebeveiliging gedefinieerd en vastgelegd, en toegepast in de vorm van functiebeschrijvingen.	ISO 27002:2013 §6.1.1
	Risicoanalyse	
1.4	De leverancier voert ten minste iedere 3 jaar een risicoanalyse uit om de bedreigingen en kwetsbaarheden, de gevolgen daarvan voor de organisatie en de kans op die gevolgen in kaart te brengen. Op basis van de risicoanalyse worden adequate beveiligingsmaatregelen vastgesteld en ingevoerd.	ISO 27001:2013 §8.2
1.4 HOOG	De leverancier voert ten minste **ieder jaar** een risicoanalyse uit om de bedreigingen en kwetsbaarheden, de gevolgen daarvan voor de organisatie en de kans op die gevolgen in kaart te brengen. Op basis van de risicoanalyse worden adequate beveiligingsmaatregelen vastgesteld en ingevoerd.	ISO 27001:2013 §8.2
1.5	De leverancier beschrijft hoe de geïdentificeerde risico's worden behandeld en onderbouwt waarom eventuele restrisico's worden geaccepteerd.	ISO 27001:2013 §8.2
	Bewustzijn en training	
1.6	Alle werknemers van de leverancier en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, krijgen training bij indiensttreding en vervolgens regelmatig bijscholing over het Informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures.	ISO 27002:2013 §7.2.2
1.6 HOOG	Alle werknemers van de leverancier en, voor zover van toepassing, ingehuurd personeel en externe gebruikers krijgen training bij indiensttreding en vervolgens **tenminste jaarlijks** bijscholing over het Informatiebeveiligingsbeleid en de informatiebeveiligingsprocedures.	ISO 27002:2013 §7.2.2
	Incidentenbeheer en datalekken	
1.7	De leverancier voert incidentenbeheer procesmatig uit. De activiteiten classificeren, prioriteren, diagnosticeren, communiceren en dossiervorming worden daarbij onderscheiden.	ISO 27002:2013 §16.1.1

1.8	De leverancier heeft functiebeschrijvingen in gebruik waarin de taken met betrekking tot incidentenbeheer zijn opgenomen.	ISO 27002:2013 §16.1.1
1.9	De leverancier hanteert een vaste werkwijze en vast format voor incidentrapportages.	ISO 27002:2013 §16.1.2
1.10	De leverancier heeft een incident classificatiekader (al dan niet geautomatiseerd) naar urgentie en impact in gebruik.	ISO 27002:2013 §16.1.4
1.11	De leverancier heeft een procedure ingericht om de opdrachtgever tijdig en adequaat te informeren over potentiële datalekken waarvan hij kennis krijgt (inclusief die bij sub-verwerkers of hulpleveranciers) en documenteert bij een incident alle stappen die zijn ondernomen in het kader van de meldplicht datalekken.	AVG, art. 28.3 Beleidsregels Meldplicht Datalekken, H2.1 – 2.4 (AP)
	Wijzigingsbeheer	
1.12	De leverancier heeft een proces ingericht voor wijzigingsbeheer, bijvoorbeeld op basis van ITIL3 of ISO 20000-1.	ISO 27002:2013 §12.1.2
1.13	De leverancier test wijzigingen in een test- of acceptatieomgeving alvorens deze in productie te brengen en legt testresultaten vast.	ISO 27002:2013 §12.1.4, §14.2.6, §14.2.9
1.14	De leverancier voert wijzigingen uit in de afgesproken servicevensters en overlegt wijzigingen met grote impact voorafgaand aan realisatie met de opdrachtgever.	
1.14 HOOG	De leverancier voert wijzigingen uit in de afgesproken servicevensters en legt wijzigingen met grote impact voorafgaand aan realisatie voor aan de *Change Advisory Board.*	
1.15	De leverancier documenteert de situatie na een wijziging in de configuratiedatabase.	ISO 27002:2013 §12.4.1
	Continuïteitsbeheer	
1.16	De leverancier heeft preventieve en correctieve maatregelen ten behoeve van de realisatie van de beschikbaarheidseisen aantoonbaar getroffen.	ISO 27002:2013 §17.2
1.17	De leverancier is bekend met de single points of failure in de infrastructuur en heeft maatregelen getroffen om storingen binnen de afgesproken termijn te kunnen verhelpen.	ISO 27002:2013 §17.2
1.18	De leverancier bewaakt de beschikbaarheid en capaciteit van applicaties en systemen continu.	ISO 27002:2013 §12.1.2 en §12.1.3
1.18 HOOG	De leverancier bewaakt de beschikbaarheid en capaciteit van applicaties en systemen continu. Overschrijdingen van drempelwaarden worden tijdig gesignaleerd en gerapporteerd aan de opdrachtgever.	ISO 27002:2013 §12.1.2 en §12.1.3
1.19	De leverancier maakt back-ups conform beschikbaarheidseisen.	ISO 27002:2013 §12.3
1.20	De leverancier bewaart back-ups beveiligd off-site. Een afstand van ten minste vijf kilometer tussen primaire opslag en backup locatie is daarbij vereist.	ISO 27002:2013 §12.3
1.21 HOOG	De leverancier heeft voor de geleverde diensten continuïteits- of disaster recoveryplannen beschikbaar, actualiseert ze regelmatig en test op regelmatige basis. Opdrachtgever wordt op de hoogte gesteld wanneer de testen zijn gepland, indien er impact op de gele-	

	verde dienst kan zijn. Indien tekortkomingen worden geconstateerd, dient er een verbeterplan of nieuw plan met duidelijk omschreven acties te worden opgesteld.	
	Geheimhouding	
1.22	De leverancier heeft een geheimhoudingsovereenkomst voor werknemers en derden in gebruik.	ISO 27002:2013 §7.1.2 (a) en §13.2.4
1.23	Werknemers van de leverancier en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, die betrokken zijn bij verwerkingen van risicoklasse Midden, dienen een Verklaring Omtrent het Gedrag (VOG) over te leggen.	ISO 27002:2013 §7.1.1
1.23 HOOG	Werknemers van de leverancier en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, die betrokken zijn bij verwerkingen van risicoklasse Hoog, dienen een Verklaring Omtrent het Gedrag (VOG) over te leggen.	ISO 27002:2013 §7.1.1

2 Toegangsbeveiliging

Toegangscontrole is essentieel voor het bepalen en weten wie toegang heeft tot (gevoelige) data. Daartoe wordt aan iedere gebruiker een uniek login ID toegekend en, eventueel op basis van rollen, toegang verleend tot de data. Onder toegangscontrole vallen ook fysieke toegangscontrole en toegang tot mobiele apparatuur.

#	Maatregel	Referentie
	Fysieke toegangsbeveiliging en beveiliging van apparatuur	
2.1	IT-voorzieningen en apparatuur zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. Genomen maatregelen zijn in overeenstemming met de vastgestelde risico's.	ISO 27002:2013 §11.1 en §11.2
	Logische toegangsbeveiliging	
2.2	De leverancier heeft een beleid voor toegangsbeveiliging vastgesteld en gedocumenteerd, waarin in ieder geval is bepaald dat: • gebruikers en beheerders een unieke login ID en wachtwoord combinatie hebben, • gedeelde login ID en wachtwoord combinaties niet zijn toegestaan en • toegang voor gebruikers en beheerders beperkt is tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	ISO 27002:2013 §9.1 en §9.2.4
2.3	De leverancier heeft een beleid inzake mobiele apparatuur, waarin ten minste is opgenomen dat: • het apparaat is voorzien van toetsvergrendeling of een vergelijkbaar middel, bijv. toegang via wachtwoord, • privé en zakelijk gebruik gescheiden zijn en bedrijfsdata op het device versleuteld is.	ISO 27002:2013 §6.2.1 en §11.2.8
2.4	De leverancier richt een formeel proces in voor het beheer van toegangsrechten van gebruikers en beheerders. Het toegangsbeheerproces omvat ten minste: • het registreren van gebruikers en de aan hen toegekende rechten,	ISO 27002:2013 §9.2.1, §9.2.2, §9.2.3, §9.4.1 en §9.2.6

	• het toekennen van niet meer rechten dan nodig voor de uitoefening van taken en • het wijzigen of intrekken van die rechten bij wijziging of beëindiging van het dienstverband of contract.	
2.5	Gebruikers en beheerders worden op de hoogte gesteld van het toegangsbeveiligingsbeleid en ondertekenen een verklaring dat zij persoonlijke geheime authenticatie-informatie geheimhouden en in geval van inbreuk direct maatregelen nemen om de gevolgen te beperken.	ISO 27002:2013 §9.3.1
2.6	De leverancier controleert maandelijks of toegekende rechten juist zijn.	ISO 27002:2013 §9.2.5
2.7	Aan de hand van het toegangsbeveiligingsbeleid richt de leverancier beveiligde inlogprocedures voor systemen en toepassingen in. De inlogprocedures omvatten ten minste een sterk wachtwoord. Uit de risicoanalyse volgt of sterke authenticatie (multi-factor authentication) voor specifieke systemen of toepassingen vereist is.	ISO 27002:2013 §9.4.2, §9.4.3

3 Beheer van technische kwetsbaarheden en anti-malware

Malware kan het netwerk en systemen op diverse manieren binnendringen en misbruik maken van kwetsbaarheden. Het gebruik van antivirussoftware en het regelmatig testen van systemen en applicaties op kwetsbaarheden vermindert deze dreiging.

#	Maatregel	Referentie
	Kwetsbaarhedenbeheer	
3.1	De leverancier richt een proces in ter voorkoming van het benutten van technische kwetsbaarheden. Het proces omvat in ieder geval: • het regelmatig up-to-date houden van systemen en software (patching), • het tijdig vergaren van informatie over nieuwe kwetsbaarheden (intelligence), • het controleren van netwerk en systemen op kwetsbaarheden (vulnerability assessment), • het testen van webapplicaties, op regelmatige basis, op kwetsbaarheden (Web application scanning), • het gebruik van antivirussoftware die dagelijks wordt geactualiseerd, • beperkingen op het installeren van (ongeautoriseerde) software.	ISO 27002:2013 §12.2, §12.6.1, §12.6.2
3.1 HOOG	De leverancier richt een proces in ter voorkoming van het benutten van technische kwetsbaarheden. Het proces omvat in ieder geval:	ISO 27002:2013 §12.2, §12.6.1, §12.6.2

#	Maatregel	Referentie
	• het regelmatig up-to-date houden van systemen en software (patching), • het tijdig vergaren van informatie over nieuwe kwetsbaarheden (intelligence), • het *geautomatiseerd* controleren van programmapakketten en infrastructurele programmatuur op bekende zwakheden, • het *continu* testen van webapplicaties op kwetsbaarheden (Web application scanning) *en het uitvoeren van een penetratietest ten minste eenmaal per jaar*, • het gebruik van *anti-malware (inclusief anti-virus) software van verschillende aanbieders met verschillende engines* die dagelijks worden geactualiseerd, • beperkingen op het installeren van (ongeautoriseerde) software.	
	Intrusion Detection	
3.2	De leverancier inspecteert gegevensverkeer vanuit externe of niet-vertrouwde netwerken real-time.	ISO 27002:2013 §13.1.2
3.3 HOOG	De leverancier heeft een Intrusion Detection/Prevention Systeem dat netwerk gebaseerde aanvallen herkent op basis van signatures, protocol validatie en anomaly detection.	ISO 27002:2013 §13.1.2
3.4 HOOG	De leverancier verwijdert alle niet voor de dienst(en) noodzakelijke services op systemen en/of zet ze uit (disabled), of – indien de systeemsoftware dit niet toelaat – blokkeert de dienst(en) via gedocumenteerde filters op de meest nabijgelegen netwerkcomponent die deze filtering kan verschaffen.	

4 Vertrouwelijkheid en integriteit van gegevens, privacy

Wanneer een aanvaller de toegangscontrole weet te omzeilen moet de data goed beschermd zijn. Dit geldt zowel voor data in rust als voor data in transit. Voor de bescherming van privacygevoelige data zijn extra maatregelen gewenst.

#	Maatregel	Referentie
	Bescherming persoonsgegevens	
4.1	De leverancier beschikt over een privacybeleid of een privacyreglement dat niet ouder is dan drie jaar en voldoet aan de eisen uit de AVG.	ISO 27002:2013 §18.1.1
4.2	De leverancier heeft een privacyfunctionaris benoemd en deze is in functie.	AVG, art. 37, 38 en 39
	Versleuteling	
4.3	De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in rust in ieder geval in de volgende situaties: • op verwijderbare media (zoals extern opgeslagen back-up tapes, DVD's, geheugenkaarten en USB-sticks);	ISO 27002:2013 §10.1, §13.2, §14.1.2

	• in het opslaggeheugen van mobiele apparatuur (zoals het in- en externe geheugen van laptops, smartphones en tablets).	CBP Richtsnoer *beveiliging persoonsgegevens*, pag. 25
4.3 HOOG	De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in rust *te allen tijde*.	
4.4	End-to-end encryptie is altijd noodzakelijk, indien data die als gevoelig of kritiek is geclassificeerd getransporteerd wordt (zoals tijdens back-up). De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in beweging in ieder geval in de volgende situaties: • beheersessies over het eigen netwerk (met encryptievoorzieningen binnen de beheertools of gebruikte protocollen); • draadloze datacommunicatie; • wachtwoorden, die worden opgeslagen of verzonden.	
4.4 HOOG	End-to-end encryptie is altijd noodzakelijk, indien data getransporteerd wordt. De leverancier versleutelt vertrouwelijke gegevens, waaronder privacygevoelige informatie, in beweging *te allen tijde*.	
4.5	De leverancier maakt gebruik van verbindingsencryptie en hashing algoritmen die voldoen aan de eisen van de tijd.	Beleidsregels Meldplicht Datalekken, H7.2.3
4.6	De leverancier gebruikt hardware oplossingen (zoals smart cards en Hardware Security Module producten) die zijn gecertificeerd volgens daartoe strekkende standaards.	
4.7	De leverancier verwijdert data van af te danken apparatuur en verwijderbare media middels een secure erase alvorens af te voeren.	ISO 27002:2013 §11.2.7
4.8 HOOG	Authenticatie van gebruikers op basis van cryptografische techniek, hardware tokens of challenge/response protocollen (sterke authenticatie) vindt in ieder geval plaats in de volgende situaties: • wanneer Single Sign-On wordt toegepast; • bij toegang vanuit een onvertrouwd netwerk; • bij beheer van kritische beveiligingsvoorzieningen (zoals firewalls, Intrusion Detection and Prevention Systems en routers).	ISO 27002:2013 §10.1.1
4.9 HOOG	De leverancier stemt de geldigheidstermijn van cryptografische sleutels en certificaten af op het kritische gehalte van de toepassing met een maximum van 1 jaar.	ISO 27002:2013 §10.1.2

5 Controle en logging

Logging en het bijhouden van gebruikersactiviteit is essentieel bij het voorkomen, detecteren of minimaliseren van de impact van een inbreuk.

#	Maatregel	Referentie
5.1	De leverancier legt activiteiten die gebruikers uitvoeren op (persoons) gegevens vast in logbestanden en registreert goedgekeurde en geweigerde pogingen om toegang te verkrijgen tot bronnen van informatie.	ISO 27002:2013 §12.4.1
5.2	De leverancier beschermt logfaciliteiten en informatie in logbestanden tegen vervalsing en onbevoegde toegang.	ISO 27002:2013 §12.4.2 AVG, art. 5.1 (e)
5.3	De leverancier legt activiteiten van systeembeheerders en -operators vast en beoordeelt ze regelmatig.	ISO 27002:2013 §12.4.3
5.4	De leverancier gebruikt één referentietijdbron waarmee alle relevante informatie verwerkende systemen worden gesynchroniseerd, zodat de nauwkeurigheid van logbestanden gewaarborgd is.	ISO 27002:2013 §12.4.4
5.5	De leverancier levert aan de opdrachtgever maandelijks een rapportage waarin ten minste zijn opgenomen: • aantallen geslaagde en mislukte inlogpogingen; • data en tijden van niet succesvolle inlogpogingen; • gevraagde en verleende toegang tot gedeelde bestanden/informatie buiten de regulieren gebruikstijden; • activiteiten van beheerders; • significante gebruikershandelingen (zoals mutaties aan autorisaties, configuratieparameters en stamgegevens; afhankelijk van applicatie); • gedetecteerde malware (wormen/virussen/spyware e.d.) en storingen in de dienstverlening.	ISO 27002:2013 §15.2.1
5.6	De leverancier bewaart alle informatie in de logbestanden tenminste 3 maanden en ten hoogste 12 maanden, tenzij wettelijke verplichtingen anders voorschrijven of de logbestanden nodig zijn voor onderzoek in het kader van een (vermoed) beveiligingsincident. Gedurende die periode kan deze informatie worden ingezien door de opdrachtgever.	AVG, art. 5.1 (e)