

Richtlijn omgang met CAK data



Afdeling: ICT Expertisecentrum

Datum: 27-11-2024

Auteur: Bas Rabeling

Versie: 1.0

Wijzigingshistorie

VERSIE	DATUM	AUTEUR	OMSCHRIJVING	VERZONDEN AAN	STATUS
0.90	04-03-2024	Bas Rabeling	Eerste opzet	Security team	Draft
0.91	05-03-2024	Linda Dellouche	Review	Bas Rabeling	Draft
0.92	29-05-2024	Bas Rabeling	Opmerkingen Linda verwerkt, dataclassificatie er uit gehaald	Ehab Shaaban Linda Dellouche Marco Zevenhuizen Walter van Oostrum	Draft
0.93	21-06-2024	Bas Rabeling	Structuur aangepast inhoudelijk commentaar nog verwerken		Draft
0.94	04-07-2024	Bas Rabeling	Commentaar verwerkt	Ehab Shaaban Linda Dellouche Marco Zevenhuizen Walter van Oostrum Harry Wiltenburg Vincent Schoenmakers Eric de Wolf	Draft
0.95	06-09-2024	Bas Rabeling	Commentaar verwerkt Beveiligd mailen aangepast	Luc van Wanrooij Walter van Oostrum Wilfred van der Schaaf	Draft
0.96	08-11-2024	Bas Rabeling	Commentaar verwerkt	CIO overleg	Draft
1.0	27-11-2024	Bas Rabeling	Document vastgesteld	DWO	Final

Goedkeuringshistorie

VERSIE	DATUM	AUTORISATIE	J/N	TOELICHTING
1.0	27-11-2024	Walter van Oostrum	J	

Bijlagen en verwijzingen

VERSIE	DATUM

Inhoudsopgave

Inleiding	4
1. Verantwoordelijkheid labelen	4
1.1. Inleiding	4
1.2. Verantwoordelijkheid classificatie data in systemen	4
1.3. Verantwoordelijkheid classificatie documenten	4
1.4. Type data	5
2. Hoe ga ik als medewerker met documenten en mails om	6
2.1. Inleiding	6
2.2. Opslag en verwerking van documenten binnen het CAK	6
2.3. Wijze van verwijderen van data	7
2.4. Opslag en verwerking van documenten buiten het CAK	8
2.5. Toegang tot de documenten en het loggen hiervan	9
2.6. Mailen van documenten	10
3. Data in databases en systemen	11
3.1. Inleiding	11
3.2. Opslag en verwerking van de data binnen het CAK (on premise en IAAS).	11
3.3. Opslag en verwerking van de data buiten het CAK	12
3.4. Toegang tot de data en logging van de toegang	14
3.5. Transport van de data	15

Inleiding

Binnen het CAK worden verschillende soorten data verwerkt. Dit document beschrijft hoe er met de verschillende soorten data moet worden omgegaan, op basis van classificaties benoemd in het dataclassificatiebeleid.

1. Verantwoordelijkheid labelen

1.1. Inleiding

Voor een goedwerkende dataclassificatie is het belangrijk dat alle data en documenten worden gelabeld zodat het voor medewerkers duidelijk is welke classificatie de data heeft. Daarnaast biedt het labelen van de data de mogelijkheid om technische maatregelen in te richten om ongewenste verspreiding van gevoelige informatie tegen te gaan. De manier waarop data moet worden gelabeld zal verwerkt worden in een werkinstructie.

1.2. Verantwoordelijkheid classificatie data in systemen

De eindverantwoordelijkheid voor het labelen van data in systemen ligt bij de dataeigenaar van de systemen. In veel gevallen zat dit een regeling directeur zijn. De uitvoering hiervan kan worden gedelegeerd.

1.3. Verantwoordelijkheid classificatie documenten

De verantwoordelijkheid voor het labelen van documenten ligt bij de auteur van de documenten. Bij al bestaande documenten dan dit ook worden opgepakt door de afdeling of het team dat verantwoordelijk is voor de documenten.

1.4. Type data

In het data classificatiebeleid worden de volgende type data onderscheiden:

- Publieke data;
- Interne data;
- Vertrouwelijke data;
- Bijzonder vertrouwelijke data.

In de onderstaande tabel worden deze begrippen uitgelegd en worden er voorbeelden bij benoemd.

Type data	Beschrijving	Voorbeelden
Publieke data	Publieke data is data die bedoeld is voor het algemene publiek.	• Informatie op de publiek toegankelijke website; • Open data.
Interne data	Bij interne data gaat het om data die bedoeld is voor intern gebruik.	• Informatie op intranet; • Informatie op breed toegankelijke DWO's zoals beleid en richtlijnen.
Vertrouwelijke data	Bij vertrouwelijke data gaat het om bedrijf kritische informatie of persoonsgegevens van medewerkers of klanten.	• Persoonsgegevens van medewerkers of klanten; • Identificerende gegevens van klanten zoals het BSN; • Vertrouwelijke informatie en documenten alleen bedoeld voor een beperkte groep medewerkers, zoals auditrapportages en risico analyses; • Niet publieke data inzake aanbestedingen.
Bijzonder vertrouwelijke data	Bij bijzonder vertrouwelijke data gaat het om data die extra bescherming nodig heeft omdat het uitlekken ervan grote nadele consequenties kan hebben voor de betrokkenen of omdat de wetgever extra bescherming vereist.	• NAW-gegevens van klanten van beschermd wonen; • NAW-gegevens van familieleden van militairen; • Detentiegegevens; • Bijzondere persoonsgegevens van medewerkers of klanten.¹

¹ Zie hoofdstuk 2 van het data classificatiebeleid voor een toelichting

2. Hoe ga ik als medewerker met documenten en mails om

2.1. Inleiding

Dit hoofdstuk beschrijft hoe medewerkers met documenten en mails moeten omgaan. Hierbij wordt gekeken naar de vertrouwelijkheid van de documenten en mails. Wanneer documenten al gelabeld zijn kan worden uitgegaan van het label dat ze al hebben. Zo niet, dan kunnen ze worden gelabeld volgens het data classificatiebeleid. Mocht je vermoeden dat het document onjuist is gelabeld dan gelieve hierover contact op te nemen met de auteur of verantwoordelijke afdeling.

2.2. Opslag en verwerking van documenten binnen het CAK

Voor de opslag van documenten binnen de VDI gelden de volgende eisen:

- Publieke en interne data mogen op de persoonlijke mappen binnen de VDI worden opgeslagen.
- Bijzonder vertrouwelijke data mag alleen in afgeschermdde Digitale werkomgevingen en fileshares worden opgeslagen, hierbij mogen er geen klantgegevens in Digitale Werkomgevingen worden opgeslagen. Vertrouwelijke data met persoonsgegevens mogen alleen tijdelijk in een VDI worden opgeslagen. Na het afronden van een bewerking moeten de documenten worden verwijderd uit de VDI. Bij nieuw in te richten processen of herzieningen moet zoveel mogelijk worden voorkomen dat persoonsgegevens in de VDI moeten worden verwerkt.
- Tenslotte moeten fysieke documenten in afgesloten kasten worden bewaard inzien ze vertrouwelijke of bijzonder vertrouwelijke data bevatten.

Type data	Opslag en verwerking in persoonlijke omgeving van de VDI toegestaan	Opslag en verwerking op afgeschermdde digitale werkomgevingen toegestaan	Opslag op afgeschermdde fileshares toegestaan	Fysieke documenten moeten in afgesloten kast worden bewaard
Publieke data	Ja	Ja	Ja	Nee
Interne data	Ja	Ja	Ja	Nee
Vertrouwelijke data	Ja ²	Ja/Nee ³	Ja	Ja
Bijzonder vertrouwelijke data	Nee	Nee	Ja	Ja

² Persoonsgegevens mogen alleen tijdelijk bewaard worden op de VDI omgeving

³ De opslag van klantdata in de Digitale werkomgeving is niet toegestaan

2.3. Wijze van verwijderen van data

Voor de wijze van verwijderen van data gelden de volgende eisen. Papieren documenten moeten vanaf de classificatie Interne data en hoger worden afgevoerd via de afgesloten papierbakken bij het CAK. Digitale documenten en e-mails kunnen gewoon verwijderd worden met de delete functie. Voor het afvoeren van fysieke apparatuur en media zal een aparte richtlijn worden opgesteld. Wanneer data mag worden verwijderd staat uitgewerkt in de richtlijn bewaartermijnen.

Type data	Papier	E-mail en digitale documenten	Fysieke apparatuur
Publieke data	In papierbak	Gewoon deleten	Komt een aparte richtlijn voor
Interne data	In afgesloten papierbak bij het CAK	Gewoon deleten	Komt een aparte richtlijn voor
Vertrouwelijke data	In afgesloten papierbak bij het CAK	Gewoon deleten	Komt een aparte richtlijn voor
Bijzonder vertrouwelijke data	In afgesloten papierbak bij het CAK	Gewoon deleten	Komt een aparte richtlijn voor

2.4. Opslag en verwerking van documenten buiten het CAK

Voor de opslag en verwerking van documenten buiten het CAK gelden de onderstaande regels. Documenten met publieke en interne data mogen wereldwijd worden verwerkt behalve in landen met een offensief cyberprogramma gericht tegen Nederland of Nederlandse belangen. Vertrouwelijke en bijzonder vertrouwelijke data mag alleen worden verwerkt binnen de Europese Economische ruimte.

Alleen documenten met publieke data mogen worden ingevoerd in clouddiensten waarmee het CAK geen overeenkomst heeft. Voor clouddiensten met een overeenkomst met het CAK geldt dat alle data er verwerkt mag worden mits de omgeving voldoet aan de beveiligingseisen. Deze worden verder uitgewerkt in hoofdstuk 3.

Type document	Geografische locatie	Verwerking in clouddiensten zonder overeenkomst CAK	Verwerking in Clouddiensten met overeenkomst CAK
Publieke data	Wereldwijd ⁴	Ja	Ja
Interne data	Wereldwijd ²	Nee	Ja
Vertrouwelijke data	Europese Economische Ruimte (E.E.R)	Nee	Ja
Bijzonder vertrouwelijke data	Europese Economische Ruimte (E.E.R)	Nee	Nee, tenzij de omgeving voldoet aan de beveiligingseisen van het CAK. Deze zijn uitgewerkt in hoofdstuk 3.

⁴ Met uitzondering van landen met een offensief cyberprogramma gericht tegen Nederland of Nederlandse belangen.

2.5. Toegang tot de documenten en het loggen hiervan

Deze paragraaf beschrijft wie er toegang tot documenten kan geven en krijgen en of deze toegang moet worden vastgelegd. Voor de toegang van vertrouwelijke en bijzonder vertrouwelijke data is het belangrijk dat de personen die toegang krijgen doelbinding met de data hebben en geautoriseerd moeten zijn om deze data te mogen verwerken (zie het logisch toegangsbeveiligingsbeleid). Dit wil zeggen dat ze vanuit hun functie de data moeten kunnen raadplegen en dit alleen doen wanneer zij die data daadwerkelijk nodig hebben ('need-to-know'). Hierbij moet altijd de minimale set aan data die nodig is worden gedeeld.

Voor vertrouwelijke data moet het achteraf mogelijk zijn wie deze heeft geraadpleegd, voor bijzonder vertrouwelijke data is het belangrijk dat dit real-time kan worden gemonitord of dat er actieve procedures zijn om regelmatig te controleren wie er toegang heeft gehad.

Type document	Wie mag er toegang krijgen tot de data	Toegang verlenen door (indien geen RBAC aanwezig)	Op welke wijze moet de toegang tot de data worden gelogd
Publieke data	Iedereen	N.v.t.	Niet nodig
Interne data - documenten	Interne medewerkers Leveranciers met doelbinding Ketenpartners met doelbinding	Auteur of afdeling auteur	Niet nodig
Vertrouwelijke data	Interne medewerkers Leveranciers met doelbinding Ketenpartners met doelbinding Deel minimale set aan data die nodig is.	Leidinggevende van auteur	Bijhouden die er toegang heeft (gehad). Functionele logging noodzakelijk om achteraf te kunnen controleren wie er toegang heeft gehad.
Bijzonder vertrouwelijke data	Interne medewerkers ketenpartners met doelbinding Deel minimale set aan data die nodig is.	Data eigenaar	Bijhouden die er toegang heeft (gehad). Functionele logging noodzakelijk om achteraf te kunnen controleren wie er toegang heeft gehad. Er moeten actieve procedures zijn waarmee de rechtmatigheid van de toegang worden gecontroleerd.

2.6. Mailen van documenten

Voor het e-mail naar buiten het CAK geldt dat publieke- en interne data via reguliere CAK mail mag worden verstuurd en dat bijzonder vertrouwelijke data alleen mag worden verstuurd via de beveiligd mailen oplossing van het CAK. Vertrouwelijke data moet met de beveiligd mailen oplossing worden verstuurd wanneer er wachtwoorden worden verstuurd of wanneer er vertrouwelijke data in de bijlage staat. Wanneer er een beperkte hoeveelheid vertrouwelijke data in de mail zelf staat mag deze ook via reguliere CAK mail worden verstuurd. **Let hierbij op dat bijzondere persoonsgegevens zoals medische informatie altijd met de beveiligd mailen oplossing moeten worden verstuurd.**

Hierbij gelden de toegangseisen van paragraaf 2.4.

Type data	Mailen naar buiten het CAK	
	Standaard mail het CAK	Beveiligd mailen oplossing van het CAK
Publieke data	X	
Interne data	X	
Vertrouwelijke data	Mails met beperkte hoeveelheid vertrouwelijke data in de mail zelf (van maximaal enkele klanten).	Mails met vertrouwelijke data in bijlage(s). Versturen van wachtwoorden
Bijzonder vertrouwelijke data		X

3. Data in databases en systemen

3.1. Inleiding

Dit hoofdstuk beschrijft hoe er moet worden omgegaan met data in databases en systemen op basis van de dataclassificatie. Hierbij wordt er gekeken naar de vertrouwelijkheid van de data. Wanneer de data al is gelabeld dan worden uitgegaan van dat label. Zo niet dan kan de data worden gelabeld volgens het data classificatiebeleid. Eventueel kan hierbij gebruikt gemaakt worden van de informatie uit de BIA en DPIA.

3.2. Opslag en verwerking van de data binnen het CAK (on premise en IAAS).

Er wordt bij voorkeur gewerkt met het verwerken van berichten bij verkeer tussen systemen. Mocht er gebruik gemaakt worden van bestanden dan is het gebruik van afgeschermd fileshares toegestaan voor de uitwisseling tussen systemen. Hierbij mogen deze fileshares alleen toegankelijk zijn voor systemen en beheerders waarbij de toegang moet worden gelogd.

Voor nieuwe databases en migraties naar nieuwe versies geldt dat vertrouwelijke- en bijzonder vertrouwelijke data in databases moet worden versleuteld. Denk hierbij bijvoorbeeld aan het gebruik van Oracle Enhanced Security. Alleen met goedkeuring van security en na het nemen van vergelijkbare mitigerende maatregelen kan hiervan worden afgeweken.

Type data	Opslag op afgeschermd fileshares toegestaan	Data moet versleuteld worden opgeslagen in databases in rust
Publieke data	Ja	Nee
Interne data	Ja	Nee
Vertrouwelijke data	Ja ⁵	Ja
Bijzonder vertrouwelijke data	Ja ³	Ja

⁵ Deze fileshares mogen alleen toegankelijk zijn voor systemen en beheerders, toegang moet worden gelogd.

3.3. Opslag en verwerking van de data buiten het CAK

Voor het verwerken⁶ van de data gelden de onderstaande eisen. Publieke en interne data mag wereldwijd worden verwerkt behalve in landen met een offensief cyberprogramma gericht tegen Nederland of Nederlandse belangen. Vertrouwelijke en bijzonder vertrouwelijke data mag alleen worden verwerkt binnen de Europese Economische ruimte.

Alleen publieke data mag worden ingevoerd in clouddiensten waarmee het CAK geen overeenkomst heeft. Voor clouddiensten met een overeenkomst met het CAK geldt dat alle data er verwerkt mag worden mits de omgeving voldoet aan de beveiligingseisen. Wel geldt er voor bijzonder vertrouwelijke data dat er een extra risico analyse en aanvullende maatregelen noodzakelijk zijn welke bepaald moeten worden in een BIA en/of PIA. Hierbij moeten bijzonder vertrouwelijke data worden versleuteld met de sleutel van het CAK. Deze sleutel moet afkomstig zijn van een door een CAK beheerd sleutelhuis. Hierbij mag een cloudprovider nooit toegang tot de data kunnen krijgen.

Type data	Geografische locatie	Verwerking in clouddiensten zonder overeenkomst CAK	Verwerking in Clouddiensten met overeenkomst CAK
Publieke data	Wereldwijd ⁷	Ja	Ja
Interne data	Wereldwijd ⁵	Nee	Ja
Vertrouwelijke data	Europese Economische Ruimte (E.E.R)	Nee	Ja
Bijzonder vertrouwelijke data	Europese Economische Ruimte (E.E.R)	Nee	Ja, mits de omgeving voldoet aan de beveiligingseisen van het CAK.

⁶ Volgens de privacywet Algemene verordening gegevensbescherming (AVG) vallen in ieder geval de volgende handelingen onder het verwerken van persoonsgegevens: verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen en vernietigen.

⁷ Met uitzondering van landen met een offensief cyberprogramma gericht tegen Nederland of Nederlandse belangen.

3.3.1. Beveiligingseisen verwerking en bijzondere vertrouwelijke data in een clouddienst

Wanneer Het CAK bijzondere vertrouwelijke data in een cloudomgeving wil verwerken dan is hier altijd een aanvullende risicoanalyse voor vereist. Hierbij moet gekeken wat het risico is van het uitlekken van de data en welke mitigerende maatregelen er mogelijk zijn. Hierbij gelden minimaal de onderstaande standaard maatregelen. Alleen wanneer uit de risicoanalyse blijkt dat er een kleiner risico is of maatregelen met vergelijkbare resultaten mogelijk zijn kan hier na goedkeuring door security van worden afgeweken.

Indien het uitlekken van de data gevaar kan opleveren voor de betrokkenen dient de data versleuteld te worden met een sleutel uit het sleutelhuis van het CAK. De provider van de dienst mag nooit toegang tot de data kunnen krijgen. Dezelfde eis geldt voor (kritisch)strategische applicaties en systemen met bijzondere persoonsgegevens van meer dan 10.000 personen. Voor niet (kritisch) strategische systemen met bijzondere persoonsgegevens van minder dan 10.000 personen kan worden volstaan met een SOC2 type 2 verklaring van de leverancier, het versleutelen van de data met een sleutel uit het sleutelhuis van het CAK is ook mogelijk.

Type bijzonder vertrouwelijke data	Classificatie applicatie en grootte dataset	Vereiste mitigerende maatregel
Bijzondere persoonsgegevens	Applicatie is niet (kritisch) strategisch en de dataset en bevat bijzondere persoonsgegevens van minder dan 10.000 personen	Leverancier beschikt over een SOC2 type II verklaring of Versleuteling van data met een sleutel uit het sleutelhuis van het CAK.
Bijzondere persoonsgegevens	Applicatie is (kritisch) strategisch en/of bevat bijzondere persoonsgegevens van meer dan 10.000 personen	Versleuteling van data met een sleutel uit het sleutelhuis van het CAK. Cloudprovider mag nooit toegang tot de data kunnen krijgen.
NAW-gegevens van klanten beschermd wonen NAW-gegevens van familieleden van militairen Detentiegegevens	Voor alle typen applicaties en grootte datasets	Versleuteling van data met een sleutel uit het sleutelhuis van het CAK. Cloudprovider mag nooit toegang tot de data kunnen krijgen.

3.4. Toegang tot de data en logging van de toegang

De toegang tot de data en de vereiste logging op de toegang tot de data verschilt voor de verschillende types data. In de onderstaande tabel staat aangegeven wie er toegang tot welke type data mogen krijgen en hoe de logging op deze toegang moet worden ingericht

Voor de toegang van vertrouwelijke en bijzonder vertrouwelijke data is het belangrijk dat de medewerkers die toegang hebben doelbinding met de data hebben en geautoriseerd moeten zijn om deze data te verwerken. Dit wil zeggen dat ze vanuit hun functie de data moeten kunnen raadplegen en dit alleen doen wanneer zij die data daadwerkelijk nodig hebben ('need-to-know'). Hierbij moet altijd de minimale set aan data die nodig is worden gedeeld.

Voor vertrouwelijke data moet het achteraf mogelijk zijn wie deze heeft geraadpleegd, voor bijzonder vertrouwelijke data is het belangrijk dat dit real-time kan worden gemonitord of dat er actieve procedures zijn om regelmatig te controleren wie er toegang heeft gehad.

Type data	Wie mag er toegang krijgen tot de data	Toegang verlenen door	Op welke wijze moet de toegang tot de data worden gelogd
Publieke data	Iedereen	N.v.t.	Niet nodig
Interne data - documenten	Interne medewerkers Leveranciers met doelbinding Ketenpartners met doelbinding	Data eigenaar	Niet nodig
Vertrouwelijke data	Interne medewerkers Leveranciers met doelbinding Ketenpartners met doelbinding	Data eigenaar	Functionele logging noodzakelijk om achteraf te kunnen controleren wie er toegang heeft gehad.
Bijzonder vertrouwelijke data	Interne medewerkers ketenpartners met doelbinding	Data eigenaar	Functionele logging noodzakelijk met mogelijkheden om real-time alerts te laten zetten op het raadplegen van de data of actieve procedures waarmee regelmatig controles worden uitgevoerd.

3.5. Transport van de data

Voor het transport van data is het gebruik van encryptie verplicht voor alle typen data. Deze staat beschreven in de richtlijn digitale gegevensstromen.

Type data	Overig transport
Publieke data	Zie richtlijn digitale gegevensstromen ⁸
Interne data	Zie richtlijn digitale gegevensstromen ⁶
Vertrouwelijke data	Zie richtlijn digitale gegevensstromen ⁶
Bijzonder vertrouwelijke data	Zie richtlijn digitale gegevensstromen ⁶

⁸ Beschikbaar via: <https://dwo.cak-bz.local/sites/CAK/ciso/layouts/15/start.aspx#/>