Deliverable: Inrichting Research Drive voor bijzondere persoonsgegevens

Introductie

Voor de opslag en verwerking van onderzoeksgegevens tijdens de pilot wordt gebruikt gemaakt van SURF Research Drive. In de verwerkersovereenkomst van Research Drive wordt aangegeven dat de dienst geschikt is voor de verwerking van gewone persoonsgegevens, de beveiligingsmaatregelen zijn hier dan ook op ingericht. Wanneer de verwerkingsverantwoordelijke bijzondere categorie persoonsgegevens verwerkt op de dienst, dient zij zorg te dragen voor het nemen van aanvullende maatregelen om deze gegevens adequaat te beveiligen.

Bij de onderzoeken van Hogeschool Leiden worden mogelijk bijzondere categorie persoonsgegevens verwerkt op de Research Drive omgeving. De maatregelen die Hogeschool Leiden heeft genomen om bijzondere categorie persoonsgegevens te verwerken op de Research Drive omgeving zijn in dit document beschreven.

Informatiebeveiliging & Privacy (IB&P) binnen Hogeschool Leiden

CGA-formulier

Bij het gebruik van een nieuwe applicatie/dienst binnen Hogeschool Leiden wordt het Informatiebeveiligings- en Privacy (IB&P) proces gevolgd. De eerste stap in dit proces is het Classificatie Gegevens en Applicatie (CGA) formulier in te vullen. In dit formulier wordt onder andere geïnventariseerd welke gegevens betrokken zijn, wat je wilt bereiken, welke koppelingen nodig zijn, wie verantwoordelijk is, etc.

Daarnaast wordt in het CGA-formulier de beveiligingsclassificatie (BIV-classificatie) vastgesteld en wordt een Pre-DPIA uitgevoerd om te bepalen of een DPIA noodzakelijk is. De BIV-classificatie van Research Drive is vastgesteld op:

- Beschikbaarheid: Midden
- Integriteit: Hoog
- Vertrouwelijkheid: Hoog

Op basis van de BIV-classificatie is een set met informatiebeveiligingsmaatregelen opgesteld waar tijdens het gebruik van Research Drive aan moet worden voldaan. De waarborging van deze informatiebeveiligingsmaatregelen is beschreven in het Research Drive beheerdocument.

Data Privacy Impact Assessment (DPIA)

Op basis van de pre-DPIA in het CGA-formulier is vastgesteld dat er een DPIA moest worden uitgevoerd. Deze DPIA is gericht op de Research Drive omgeving zelf en niet op de onderzoeken. Wanneer uit de CGA-formulieren van de individuele onderzoeken blijkt dat er een DPIA moet worden uitgevoerd zal er voor het onderzoek een DPIA worden opgesteld.

Configuratie Research Drive

Hogeschool Leiden maakt gebruik van een Institutional (branded) instance van Research Drive, hierbij kunnen verschillende policies worden ingesteld evenals aanvullende configuraties. De ingestelde policies en configuratie op de Research Drive instance van Hogeschool Leiden zijn in de onderstaande tabellen beschreven:

Policy	**Invulling hogeschool Leiden**
Accounttypes	SURFconext & local
Federated login	SURFconext
Retention periode (trashbin)	30 days
Retention period (versions)	14 days
Jupyter notebook	Enabled
Collaborative editing	Enabled
Password policy (general)	Enforce 1 lowercase, 1 uppercase, 1 number and special characters, enforce a minimum length of 10 characters.
Password policy (users)	Last 2 passwords should not be used Force user to change their password on first login
Password policy (public links)	14 days maximum until link expires if password is set

General Configuration

Option	**Invulling hogeschool Leiden**
External Storage Types	WebDAV
Allow sharing of external storage folders	Enabled
Offer client downloads on first login	Enabled

Sharing configuration

Option	**Invulling hogeschool Leiden**
Allow public links	Enabled (in overleg mogelijk uitschakelen)
Enforce public link passwords	Enabled
Public link expiration	14 days until link expires if password is set
Allow emailing public links	Enabled
Allow sharing via social media	Disabled
Allow file drop functionality	Enabled

Shares

Option	**Invulling hogeschool Leiden**
Automatically accept local shares	Enabled (na de pilotperiode uitschakelen)
Allow resharing	Enabled (na de pilotperiode uitschakelen)
Allow sharing with groups	Enabled
Restrict to users in own groups	Disabled
Restrict to own groups	Disabled
Allow mail notifications for shares	Enabled
Allow user name auto-completion in share dialog	Enabled
Federated sharing creations	Enabled
Federated sharing acceptation	Enabled

Beveiligingsmaatregelen genomen door SURF

In de Verwerkersovereenkomst heeft SURF een overzicht gegeven van de technische en organisatorische maatregelen die worden genomen bij SURF Research Drive. Enkele van deze maatregelen zijn*:

Technische maatregelen

- Strikte toegangsprocedure tot gebouwen en het datacenter
- Data is in rust versleuteld
- Gebruikers worden gewezen op de mogelijkheid om data aan de client kant ook te versleutelen
- Research Drive ondersteunt 2-factor authenticatie middels Secure-id en/of TOTP. Dit wil zeggen dat naast kennis (gebruikersnaam en wachtwoord) de gebruiker ook nog wordt gecheckt op het bezit (SMS, token) Deze optie kan op verzoek van de klant worden ingeschakeld.

Organisatorische maatregelen

- Security organisatie is opgezet en de rollen en verantwoordelijkheden zijn toegekend.
- Rollen en rechtenmodel (autorisatiematrix) wordt periodiek geëvalueerd
- Verwerker is ISO 27001 gecertificeerd

*Een overzicht van alle technische en organisatorische maatregelen is beschikbaar in de Verwerkersovereenkomst.

Aanvullende (beveiligings)maatregelen

Naast de door SURF genomen beveiligingsmaatregelen en de maatregelen uit de IB_maatregelenset kan er gebruik worden gemaakt van een aanvullende (beveiligings)maatregel. Deze maatregel wordt op de SURF Research Drive Wiki beschreven en betreft een maatregel waarbij gegevens voordat deze naar de Research Drive worden geüpload worden geencrypt met behulp van Cryptomator. Deze versleutelde gegevens kunnen vervolgens met behulp van de OwnCloud Desktop Client worden overgezet naar Research Drive. Deze maatregel wordt nu kort verder toegelicht.

OwnCloud Desktop Client

De OwnCloud Desktop Client is een applicatie die de onderzoeker kan gebruiken om onderzoeksgegevens te uploaden naar de Research Drive omgeving en bestanden te synchroniseren tussen de eigen desktop en de Research Drive omgeving. Door deze synchronisatie zijn de bestanden zowel op de desktop van de gebruiker als op de Research Drive omgeving beschikbaar.

Cryptomator

Cryptomator is een Open Source desktopapplicatie waarmee gegevens kunnen worden versleuteld met behulp van AES-encryptie.

Werkwijze Cryptomator en de OwnCloud Desktop Client

Cryptomator werkt aan de hand van Vaults (beveiligde mappen) die zijn beveiligd met een wachtwoord. Alle mappen en bestanden die in de Vault worden geplaatst worden vervolgens geencrypt met AES-encryptie.

Door de Vault vervolgens te plaatsen in de op de desktop gesynchroniseerde map (van de OwnCloud Desktop Client) wordt de Vault met de versleutelde gegevens geüpload naar de Research Drive omgeving. De gegevens zijn nu in versleutelde vorm beschikbaar op de Research Drive omgeving.

Gebruikers kunnen Vaults onderling delen door de Vault te selecteren in de Research Drive omgeving en deze toe te voegen aan de Cryptomator applicatie. Wanneer een gebruiker het wachtwoord van de Vault invoert komen de gegevens beschikbaar in de applicatie van de gebruiker.

Voor- en nadelen

Deze werkwijze levert de volgende voor- en nadelen op:

Voordelen:

- Aanvullende beveiliging voor gegevens op de Research Drive omgeving, mogelijk een invulling voor het werken met hoog-geclassificeerde/bijzondere gegevens.

Nadelen:

- Voor het uploaden van Vaults, met daarin de versleutelde gegevens, is de OwnCloud Desktop Client benodigd. Bij het gebruik van de OwnCloud Desktop Client worden de gegevens gesynchroniseerd tussen de desktop van de gebruiker en de Research Drive omgeving. Hierdoor zijn de gegevens zowel op het device van de gebruiker als op Research Drive beschikbaar.
- Bij verlies van het wachtwoord van de Vault en bij verlies van de Recovery Key zijn de versleutelde onderzoeksgegevens niet meer toegankelijk. Dit is ook voor de support afdelingen niet meer te herstellen.

Conclusie

Op basis van de IB_maatregelenset (afkomstig van het CGA-formulier), de uitgevoerde DPIA voor Research Drive en de maatregel beschreven op de Research Drive wiki is samen met het Loket Privacy besloten dat onder de volgende voorwaarden bijzondere categorie persoonsgegevens mogen worden opgeslagen/verwerkt op Research Drive:

- <u>Multi-Factor Authenticatie (MFA) is ingeschakeld voor inloggen op de Research Drive omgeving.</u>
  Zowel bij hogeschool Leiden gebruikers (organisatieaccount) als bij externe gebruikers (lokaal Research Drive account) dient MFA te zijn ingeschakeld:
  - *Organisatieaccount:* Gebruikers met een organisatieaccount loggen in op Research Drive door middel van SURFconext, hierbij wordt MFA afgedwongen.
  - *Lokaal Research Drive account:* Externe gebruikers krijgen veelal toegang door middel van een lokaal Research Drive account, een gebruiker dient hierbij MFA zelf in te stellen. Hiervoor is een instructie opgesteld die bij de e-mail uitnodiging aan de gebruiker wordt verzonden.

- <u>De gegevens worden vooraf door de gebruiker geencrypt voordat deze op de Research Drive omgeving worden opgeslagen</u>
  De gegevens worden hierbij geencrypt met behulp van Cryptomator en door middel van de OwnCloud Desktop Client naar de Research Drive omgeving geüpload.

  EN/OF

- <u>De gegevens zijn gepseudonimiseerd opgeslagen op de Research Drive omgeving, hierbij is de sleutel opgeslagen op een andere locatie.</u>
  Een tweede optie is om de gegevens te pseudonimiseren, hierbij worden de gepseudonimiseerde gegevens opgeslagen op de Research Drive omgeving en wordt de sleutel opgeslagen op een andere locatie.