DLM Standard Operating Procedure Gegevensbeheer

Versie mei 2020 De Lerende Mens B.V.
De Lerende Mens B.V. is gevestigd te Nijmegen met Kamer van Koophandelnummer 71942068.

In dit document staat vermeld hoe De Lerende Mens B.V. (DLM) de procedures van databeheer heeft ingericht.

In het separate document DLM Document Persoonlijke Data staat vermeld wat persoonlijke data is voor DLM en waarom DLM welke noodzakelijke informatie verzamelt en bewaart.

Beide documenten zijn onlosmakelijk verbonden met DLM Algemene Privacyverklaring en DLM Algemene Voorwaarden. Alle documenten staan op www.delerendemens.nl.

Doel

Het doel van dit document is om met de hierin vastgelegde afspraken te waarborgen dat DLM zorgdraagt voor een optimaal databeheer van data en persoonlijke gegevens dat veilig en in overeenstemming met de privacywetgeving is.

Basisprincipes

- Alle persoonlijke data moeten op afzonderlijke locaties worden opgeslagen, met regelmatige automatische back-ups,
- Alle persoonlijke data moeten worden vastgelegd en opgeslagen met niet-identificeerbare onderwerp codes,
- Als persoonlijke data worden opgeslagen, mogen ze alleen worden opgeslagen als onderdeel van een pseudonimisatiesleutel, een bestand dat niet-identificeerbare onderwerpcodes koppelt aan de persoonlijke gegevens van elke deelnemer (bijvoorbeeld in een tabel),

- Pseudonimisatiesleutels moeten altijd worden opgeslagen op een locatie die is beveiligd met een sleutel (bijvoorbeeld een wachtwoord). Deze sleutel is alleen bekend bij de personen die deze nodig hebben voor hun werk,
- Sleutels moeten zo worden opgeslagen dat ze niet toegankelijk zijn voor onbevoegde personen,
- Gegevens moeten spaarzaam worden opgeslagen, op niet meer locaties dan nodig,
- Communicatie over privacygevoelige gegevens gebeurt via beveiligde kanalen (onder meer via telegram en de Asgaard Saga portal).

Implementatie

De volgende onderzoeksfasen worden onderscheiden:

1. **data-acquisitie,**
2. **data-analyse,**
3. **data-uitwisseling met externe partijen.**

Richtlijnen voor het delen van data binnen DLM binnen fase 1 en 2 data worden hierna gegeven.

1. Data-acquisitie

Voor het werken

- De pseudonimisatiesleutel moet worden opgeslagen op een extra beveiligde locatie. Als meerdere personen toegang moeten hebben, is er een beperkte, gecontroleerde toegang,
- Het is niet toegestaan pseudonimisatiesleutels op meerdere locaties op te slaan. Meerdere backups valt hier buiten,
- De data van Asgaard Saga moeten via een beveiligd netwerk protocol worden overgedragen,
- De gegevens moeten worden opgeslagen op servers binnen Europa,
- Voor het bewaren van data worden de richtlijnen van Radboud Universiteit gevolgd,
- De backups van persoonlijke data worden bewaard op drie verschillende locaties door hiervoor gekwalificeerde partijen.

2. Data-analyse

Voor het werken

- De data analist heeft alleen bezit over de data, niet de persoonsgegevens,
- Voor gegevensanalyse is het soms vereist dat de gegevens dicht bij de computer worden opgeslagen, wat data-analyse mogelijk maakt. Het is toegestaan om tijdelijke kopieën van de data naar andere locaties te maken, mits deze locaties minimaal met een wachtwoord zijn beveiligd. Deze gegevens moeten van deze locaties worden verwijderd zodra de analyses zijn uitgevoerd,
- Lokale harde schijf van de computer: als deze schijf op zichzelf niet met een wachtwoord is beveiligd, is deze schijf mogelijk ook toegankelijk voor andere gebruikers. Als de data geen persoonlijke kenmerken bevat, kan de data worden opgeslagen zonder verdere extra encryptiemaatregelen,
- Laptop: deze dient een sleutel beveiligd gebruikersaccount te hebben en er moet van gecodeerde harde schijven gebruikt worden gemaakt,
- DLM werkt vanuit een beveiligde opslag. Op dit moment is dit Surfdrive.

Voor archivering

- Originele data en de bijbehorende scripts / equivalente bestanden die de geanalyseerde resultaten opleveren, worden opgeslagen.

3. Data-uitwisseling met externe partijen

Voor het werken

- Pseudonimisatiesleutel kan nooit worden gedeeld met de externe gemeenschap.

Voor archivering

- Gegevens die persoonlijke data bevatten, moeten worden geanonimiseerd, tenzij deelnemers expliciet toestemming hebben gegeven voor het delen van deze persoonlijke data, bijvoorbeeld scholen.

Data-uitwisseling binnen DLM

Tijdens data-acquisitie en data-analyse

- Data kunnen worden gedeeld binnen DLM, mits dit op een veilige manier gebeurt. Voor het delen van data wordt een beveiligde omgeving aanbevolen (op dit moment telegram),

- Het delen van persoonlijke data extern en binnen DLM moet tot het minimale beperkt worden. Persoonlijke data staat op een locatie met extra encryptie,
- Als data worden benaderd vanaf externe locaties, moet een beveiligde verbinding worden gebruikt. Het apparaat van waaruit gegevens worden benaderd, moet veilig zijn,
- Data moeten digitaal worden overgedragen (en niet op draagbare opslagmedia).

Reikwijdte

- Deze procedure is van toepassing op alle verzamelde (persoonlijke) data waarvan DLM de rechthebbende is,
- Deze procedure omvat verantwoordelijkheden voor alle medewerkers van DLM: vrijwilligers, assistenten, data-analisten, technisch en administratief personeel en alle aangewezen medewerkers die data verzamelen en / of verwerken,
- Een Standard Operating Procedure (SOP) is een schriftelijk document of instructie waarin alle stappen en activiteiten worden beschreven die moeten worden genomen om uniformiteit van de uitvoering te bereiken.

Wijzigingen

Wijzigingen zullen minimaal één maand van te voren aangekondigd worden op www.delerendemens.nl.