Naam document: Procedure - Datalek	Proceseigenaar : Operationeel Manager
Documentnummer: 3.1.6.3	Procesbeheerder: Operationeel Manager
	Datum vaststelling: 01-02-2021
	Datum laatste wijziging:

1. **DOELSTELLING**
   Dit document beschrijft de handelingen te verrichten door Samen Top bij een datalek. Het doel van dit document is vastleggen welke stappen genomen moeten worden door Samen Top bij een vermoeden of kennisneming van een incident dat (mogelijk) aangemerkt kan worden als datalek.

2. **TOEPASSINGSGEBIED**
   De procedure is van toepassing op de gehele organisatie van Samen Top, maar wordt uitgevoerd door de verwerkingsverantwoordelijke van Samen Top.

3. **DEFINITIES**
   Betrokkene: degene op wie een persoonsgegeven betrekking heeft.

   Bewerker: degene die ten behoeve van Stichting Samen Top persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

   Bijzondere persoonsgegevens: persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, strafrechtelijke persoonsgegevens en persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag.

   Cliënt: een persoon, zijn ouder(s) of stiefouder of anderen die de persoon als behorend tot hun gezin verzorgen en opvoeden en die is of zijn aangemeld bij Centrum Indicatie Stelling (CIS).

   Dossier: elk op naam van de client/personeel gestructureerd geheel van persoonsgegevens, dat volgens bepaalde criteria toegankelijk is, en dat betrekking heeft op de client/personeel alsmede op verschillende personen die in relatie staan tot deze personen, waarbij de persoonsgegevens op geautomatiseerde wijze worden verwerkt.

   Persoonsgegevens: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

   Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

Verstrekken van persoonsgegevens: het bekend maken of ter beschikking stellen van persoonsgegevens.

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

AVG: Algemene Verordening Gegevensbescherming, welke vanaf mei 2018 van kracht is. De AVG gaat over het rechtmatig omgaan met persoonsgegevens, welke alleen verwerkt mogen worden in overeenstemming met deze wet. Persoonsgegevens mogen alleen verzameld worden met een gerechtvaardigd doel. Dat doet moet welbepaald zijn en vooraf uitdrukkelijk zijn omschreven. Het doel waarvoor de organisatie de persoonsgegevens gaat verwerken moet verenigbaar zijn met het doel waarmee de persoonsgegevens zijn verzameld. Uitgangspunt hierbij is ‘zo min mogelijk’

Verwerkingsverantwoordelijke: persoon welke verantwoordelijk is voor het verwerken van desbetreffende persoonsgegevens. Deze persoon zorgt ervoor dat de gegevens juist zijn en zo nodig worden geactualiseerd.

Beveiliging: De gegevensverwerking moet op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

Datalek: een inbreuk op de beveiliging waarbij persoonsgegevens per ongeluk of op onrechtmatige wijze in handen van onbevoegden zijn gekomen, voor onbevoegden toegankelijk waren, of zijn vernietigd, gewijzigd of verloren.

FG – Functionaris gegevensbescherming
DC – Datalek commissie
AP – Autoriteit persoonsgegevens

4. RISICO’S

- Wanneer er onjuist gehandeld wordt na het constateren van een datalek, kan dat ernstige schade veroorzaken aan de privacy van cliënten van Samen Top
- Wanneer datalekken niet tijdig gesignaleerd worden, kan dat ernstige schade veroorzaken aan de privacy van cliënten van Samen Top

5. DOCUMENTEN

Document	Omschrijving document
Beleid – Privacy en gegevensbescherming	Document waarin het beleid en de visie van Samen Top op het omgaan met persoonsgegevens beschreven staat

6. PROCEDURE

No	Korte beschrijving van processtap + functie uitvoerder	Uitvoerder, werkwoord, tijd en registratie (hyperlink naar onderliggende documenten)
1	Identificeren data lek (betrokken medewerkers)	Betrokken medewerkers signaleren een data lek en koppelen dat direct door aan het MT van Samen Top middels het meldingssysteem in Sharepoint op de pagina 'Privacy'
2	Beoordelen aard/ ernst incident (Management)	Management krijgt melding en beoordeeld de aard en de ernst van het incident samen met de Functionaris Gegevensbescherming. Zij bepalen of er sprake is van een data lek. In overleg kunnen zij direct overgaan tot maatregelen of onderstaande stappen volgen. Daarnaast bepalen zij of het data lek gemeld dient te worden aan de politie.
3	Er wordt melding gemaakt aan de Autoriteit Persoonsgegevens (management)	Management maakt indien sprake van een datalek melding aan de Autoriteit Persoonsgegevens op basis van het Beleid – Privacy en gegevensbescherming. Dit gebeurt binnen 72 uur na het melden van het data lek via het online meldingsformulier op de website van AP. https://autoriteitpersoonsgegevens.nl/
4	Instelling Datalekken Commissie (MT)	Management stelt een commissie van ten minste drie leden op voor het opstarten, verwerken en afronden van de melding. Betrokkenen in de situatie rondom het data lek kunnen hier niet aan deelnemen.
5	Startbijeenkomst Datalekken Commissie (MT)	Eerste bijeenkomst met commissie, waarin de situatie besproken wordt en het onderzoek wordt voorbereidt. MT draagt zorg voor het delen van alle beschikbare informatie.
6	Verrichten data lek onderzoek (DC)	Commissie verricht een onderzoek naar het ontstaan van het data lek en hoe dit in de toekomst voorkomen kan worden. Bevoegdheden van de commissie:

		- Mogelijkheid om iedereen te spreken - Alle relevante documenten in te zien - Toegang te hebben tot alle plaatsen - In relatie tot de externe bewerker gelden de afspraken zoals vastgelegd in de verwerkersovereenkomst. Het onderzoek is binnen 4 weken na melding afgerond.
7	Beoordeling melding aan betrokkenen	De beoordeling stelt vast op voorwaarde van Beleid – Privacy en gegevensbescherming of betrokkenen geïnformeerd dienen te worden over het incident.
8	Slotbijeenkomst vaststellen rapport (DC)	Maximaal 6 weken na de melding aan AP vindt deze slotbijeenkomst plaats en wordt geëvalueerd of alles goed afgehandeld is en risico's in de toekomst voorkomen worden
9	Rapporteren aan betrokkenen (DC)	In samenspraak met MT en FG stelt de commissie een informatiedocument op wat teruggekoppeld kan worden aan betrokkene.
10	Implementeren verbetermaatregelen (MT)	Het MT is verantwoordelijk voor het doorvoeren en implementeren van verbetermaatregelen en ziet er op toe dat de communicatie rondom en de uitvoering van de verbetermaatregelen goed verloopt en tijdig wordt geëvalueerd.
11	Sluiten melding en vastlegging (MT)	MT informeert alle betrokken personen in bovengenoemde stappen over het sluiten en afronden van de melding.