College van bestuur

Open Universiteit

[redacted]

E: cvb@ou.nl

UITSLUITEND PER E-MAIL VERZONDEN:

[redacted]

29 april 2024
Uw Woo-verzoek d.d. 30 maart 2024

ons kenmerk: U2024/3316 HUM/JNI

Geachte [redacted]

Naar aanleiding van uw verzoek op grond van de Wet open overheid d.d. 30 maart 2024 berichten wij u als volgt.

U vraagt om de onderstaande informatie met betrekking tot (vermeende) datalekken van de Open Universiteit.

1. Alle in documenten vastgelegde communicatie over concrete gevallen van (vermeende) datalekken die zich in de periode 1 januari 2020 t/m 31 december 2021 bij uw organisatie hebben voorgedaan. Bijvoorbeeld: een e-mail van een medewerker waarin melding wordt gemaakt van een (vermeend) datalek, notulen van overleggen waarin (vermeende) datalekken worden besproken, meldingen aan de Autoriteit Persoonsgegevens, terugkoppeling van de Autoriteit Persoonsgegevens, melding naar persoon waarop het datalek ziet, een extern advies over een concreet (vermeend) datalek, het datalekregister etc.
2. Documenten ten aanzien van procedures en beleid ten aanzien van datalekken
3. Audits ter voorkoming van datalekken.

Op 12 april 2024 heeft u ons ter specificering het volgende laten weten:

'Audits ter voorkoming van datalekken' zijn onderzoeken, intern of extern, die tot doel hebben datalekken te voorkomen. Dat kan zijn door een interne toezichthouder, een extern bureau, een ICT-bedrijf etc. Technische wetenwaardigheden die de veiligheid van de OU in gevaar brengen, mogen worden weggelakt.
Voor punten 2 en 3 geldt de afbakening van 1 januari 2020 t/m 31 december 2021 niet. Om het overzichtelijk te houden mag u documenten van voor 1 januari 2014 buiten beschouwing laten'.

Wij verwijzen per vraag/vragen naar de betreffende bijlagen.

bezoekadres: Valkenburgerweg 177 Heerlen
postadres: Postbus 2960 6401 DL Heerlen
T 045 - 576 22 22

Open Universiteit

Ad 1.
Wij verwijzen u voor het overzicht van kalenderjaar 2020 en 2021 naar het bijgevoegde overzicht van (vermeende) datalekken, inclusief de gevraagde correspondentie hierover.

Toelichting. De Open Universiteit registreert informatiebeveiligingsincidenten en datalekken in één overzicht. Dit overzicht wordt met name bijgewerkt door de Functionaris Gegevensbescherming en Chief Information Security Officer. Het totaaloverzicht per kalenderjaar bevat zowel incidenten die worden aangemerkt als een datalek als incidenten die betrekking hebben op informatiebeveiliging (niet zijnde een datalek). Tevens is per kalenderjaar een overzicht bijgevoegd met een zaaknummer per datalek waarnaar wordt verwezen in verband met de beantwoording van uw verzoek. U ontvangt van ons het overzicht en per zaaknummer de door u gevraagde correspondentie.

De Open Universiteit heeft ca. 880 medewerkers en is in vergelijking met de ander universiteiten een relatief kleine organisatie. Dat blijkt ook uit het aantal medewerkers waarbij de taken en verantwoordelijkheden die voortvloeien uit de AVG worden belegd. De Open Universiteit heeft een Functionaris Gegevensbescherming, een Chief Information Security Officer en een Privacy Officer, die - afhankelijk van de aard en omvang van het datalek - worden betrokken bij de behandeling en afhandeling van datalekken. De lijnen zijn kort, afstemming vindt vaak mondeling plaats (via Teams en/of telefonisch), ook met de gemandateerde verwerkingsverantwoordelijke en het College van bestuur (in geval van een datalek met een hoog risico). Hierdoor is de verslaglegging en/of correspondentie in sommige gevallen beperkt.

Ten behoeve van deze vraag zijn de bijlagen genummerd met het zaaknummer.

Ad 2.
Wij verwijzen u voor procedures en beleid ten aanzien van datalekken naar de bijlagen. Het betreft externe en interne (voor medewerkers) toegankelijke informatievoorziening.

Ten behoeve van deze vraag zijn de bijlagen genummerd met het begincijfer 2.

Ad 3.
De beantwoording van deze vraag over de audits laat zoals aangegeven langer op zich wachten; de Open Universiteit is in sommige gevallen genoodzaakt om eerst zienswijzen op te vragen voordat we deze informatie openbaar kunnen maken.

Volledigheidshalve merken wij ten aanzien van onze beantwoording op deze vraag wel alvast het volgende op.

De Open Universiteit maakt gebruik van IT-systemen in eigen beheer (on-premises) en van Cloud oplossingen (SaaS). De systemen in eigen beheer kunnen in opdracht van de Open Universiteit worden ge-audit, de cloud applicaties worden ge-audit door de leverancier. Daarnaast zijn beide onderdeel van de Surfaudit. De centrale informatiesystemen rondom aanmelden en toelaten (inclusief infrastructuur, identity- & accessmanagement, etc.) zijn onderdeel van het jaarlijkse Logius beveiligingsassesment.
Met elke verwerker wordt voorts een verwerkersovereenkomst gesloten met relevante verwerkings- en contactinformatie.

Open Universiteit

Uiteraard kunnen datalekken hiermee niet geheel worden voorkomen maar de Open Universiteit spant zich maximaal in om ze te voorkomen en om, als ze er onverhoopt toch zijn, correct te handelen om eventuele schade te beperken.

Met vriendelijke groeten.

Dr. Nicole Ummelen
voorzitter