Protocol Privacy voor medewerkers Bureau KNHG

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat er vanaf die datum dezelfde privacywetgeving geldt in de hele Europese Unie (EU). Als organisatie die werkt met persoonsgegevens legt deze wet KNHG een aantal verplichtingen op. Tevens komt er meer nadruk te liggen op de verantwoordelijkheid van organisaties zoals KNHG om aan te tonen dat wij ons aan deze wet houden, de zogenaamde verantwoordingsplicht. Dit geldt zowel op technisch als op organisatorisch gebied.

Als verenigingsbureau komen de medewerkers/vrijwilligers/staigair(e)s van KNHG in aanraking met privacygevoelige gegevens. Dit zijn persoonsgegevens van bijvoorbeeld leden en deelnemers aan congressen en evenementen die het KNHG organiseert. Daarom raakt de AVG direct aan het werk van medewerkers, vrijwilligers en stagiair(e)s van KNHG. Dit protocol beschrijft wat het KNHG van zijn medewerkers verwacht, zowel inhoudelijk als wat werkhouding betreft.

Geheimhouding

Medewerkers/vrijwilligers/stagiair(e)s van KNHG hebben geheimhouding wanneer zij werken met of in hun werk kennis kunnen nemen van persoonsgegevens.

Werkhouding

Medewerkers/vrijwilligers/stagiair(e)s moeten zich te allen tijde bewust zijn dat op computers/schrijven/mailboxen privacy gevoelige informatie bevindt én dat in het dagelijkse werkverkeer zij in aanraking kunnen komen met persoonsgegevens, of deze kennis kunnen verkrijgen. Dit vereist discipline in de omgang met deze data. In een collegiale werksfeer is het van groot belang dat medewerkers elkaar, vriendelijk doch doordrongen van de urgentie, aanspreken op deze discipline.

Maatregelen

Er wordt van medewerkers/vrijwilligers/stagiair(e)s verwacht dat:

- Computers ‘’gelocked’’ zijn wanneer medewerkers/vrijwilligers/stagiair(e)s weglopen van hun bureau;
- Er geen documenten met privacy gevoelige info (zoals bijvoorbeeld deelnemerslijsten, mails met daarin info van leden etc) slingeren op bureaus of in vergaderzalen of in prullenbakken gestopt worden. Er is een papiervernietiger op het bureau aanwezig waarmee deze documenten vernietigd kunnen worden;
- Medewerkers een zogenaamd ‘clean desk’ beleid voeren. Dat wil zeggen alles wat persoonsgegevens of andere privacygevoelige informatie bevat, op een afsloten plek (in bureaulades of kasten waarbij deze lades/kasten aan het einde van de werkdag ook afgesloten worden) bewaard wordt;
- Stagiair(e)s en vrijwilligers werkzaam in flexkamers (of andere ruimtes die niet afsluitbaar zijn en waar ook geen afsluitbare bureaulades tot de beschikking staan) moeten alertheid betrachten wanneer zij hun flexplek verlaten. Neem dan de privacygevoelige informatie mee of berg het eerst op in het kantoor van KNHG;
- Als de privacygevoelige informatie niet langer nodig is, er in overleg met de directeur KNHG wordt besloten of de informatie bewaard moet worden (conform de wettelijke

bewaartermijnen) of vernietigd moet worden. In het laatste geval moet deze informatie of digitaal verwijderd worden en alle schriftelijke versies/kopieën vernietigd worden m.b.v. de papierversnipperaar;
- In het geval er grote(re) groepen gemaild worden, worden de e-mailadressen van de ontvangers te allen tijde in de BCC-aanhef geplaatst zodat de privacy van de ontvangers gewaarborgd is;
- Persoonsgegevens (van medewerkers, relaties of leden) worden niet verstrekt aan derden.

Werken op afstand

Er wordt van medewerkers/vrijwilligers/stagiair(e)s verwacht dat:

- Wanneer medewerkers/vrijwilligers/stagiair(e)s op afstand werken – m.b.v. Citrix of via webmail –zich ervan vergewissen dat het netwerk waarop zij werken veilig is.
- Wanneer het netwerk niet veilig is, is het niet toegestaan om met Citrix op afstand te werken. Tevens is het van belang dat zij bewust zijn van hun omgeving (kan er iemand meekijken?);
- Als het noodzakelijk is om documenten te downloaden op computers of per email te versturen, dat alleen is toegestaan wanneer deze geen persoonsgegevens bevatten;
- Voor het gebruik van privé laptops, ipads, usb-sticks, mobiele telefoons of andere digitale gegevensdragers geldt, dat deze uitgezet of gelocked moeten worden, wanneer er niet langer op afstand gewerkt wordt zodat er niet ingebroken kan worden;
- In het geval het gebruik van data opslag bij cloud toepassingen (dropbox, google docs etc.) is het niet toegestaan, persoonsgegevens te verzamelen en op te slaan. Deze informatie mag alleen op een beveiligde omgeving toegevoegd, bewerkt en opgeslagen worden op de servers van het HuC waar het KNHG schijfruimte heeft;
- Er geen documenten met privacy gevoelige info (zoals bijvoorbeeld deelnemerslijsten, mails met daarin info van leden etc) slingeren op plekken waar op afstand gewerkt wordt.

Datalekken

Wanneer een datalek geconstateerd wordt binnen het KNHG, meldt de betrokken medewerkers/vrijwilligers/stagiair(e)s dit onverwijld bij de directeur KNHG. Deze informeert per direct de voorzitter van het bestuur en de Autoriteit Persoonsgegevens. Tevens worden onmiddellijk de noodzakelijke (technische) stappen ondernomen om het datalek te dichten.

Ondertekening

Medewerkers die in dienst zijn van KNHG ontvangen dit protocol in tweevoud en ondertekenen dit uiterlijk 25 mei 2018 . Vrijwilligers/staigair(e)s van KNHG ontvangen bij aanvang van hun stage/indiensttreding dit protocol in tweevoud. Op hun eerste werkdag leveren zij een exemplaar ondertekend retour aan directeur KNHG die deze documenten in een aparte map bewaart op een afgesloten plek op het kantoor van KNHG.

Actualisering

Dit protocol is op 8 mei 2018 opgesteld en op 23 mei geactualiseerd.

Hierbij verklaar ik …….. dat ik op …… dit protocol heb ontvangen, begrepen en voor akkoord heb ondertekend.