Privacy Protocol for KNHG Bureau staff

On 25 May 2018 the General Data Protection Regulation (GDPR) came into force. This means that from that date onward the same privacy legislation applies throughout the European Union (EU). As an organization that handles personal data, the KNHG is subject to various obligations pursuant to this law. In addition, organizations such as the KNHG have an increased responsibility to show that we comply with this law, known as the accountability requirement. This holds true for both technical and organizational aspects.

As an association bureau, KNHG staff/volunteers/trainees handle privacy-sensitive data. These are personal data, for example of members and participants in congresses and events that the KNHG organizes. The GDPR therefore directly impacts the work of KNHG staff, volunteers and trainees. This protocol describes what the KNHG expects from its staff, in both substance and work ethic.

Non-disclosure

KNHG staff/volunteers/trainees have a non-disclosure obligation, if they work with or may learn of personal data in the course of their work.

Work ethic

At all times, staff/volunteers/trainees need to be aware that privacy-sensitive information is present on computers/written documents/mailboxes, *and* that they may handle personal data or may acquire such knowledge as part of their daily work. Handling these data requires discipline. While working with colleagues, it is essential that staff hold each other to this discipline kindly but with a sense of its urgent nature.

Measures

The following is expected of staff/volunteers/trainees:

- Computers should be ‘’locked’’ whenever staff/volunteers/trainees leave their desk
- No documents containing privacy-sensitive info (such as for example lists of participants, mails with info from members etc.) may be left lying about on desks or in meeting rooms or placed in rubbish bins. A paper shredder for destroying these documents is available at the bureau.
- Staff have what is known as a ‘clean desk’ policy. This means that everything containing personal data or other privacy-sensitive

information is stored in a closed place (in desk drawers or closets, where these drawers/closets can also be locked at the end of the working day).
- Trainees and volunteers working in flex rooms (or other areas that cannot be locked, and where no desk drawers that can be locked are available) must stay alert when leaving their flex station. They should take the privacy-sensitive information with them or store it at the KNHG office first.
- When the privacy-sensitive information is no longer needed, in consultation with the KNHG director, it shall be decided whether the information is to be stored (in accordance with the retention periods prescribed by law) or destroyed. In the latter case, this information must be digitally deleted, and all written versions/copies destroyed, using the paper shredder.
- When e-mails are sent to large (larger) groups, the e-mail addresses of the recipients shall always be placed in the BCC section to safeguard the privacy of the recipients.
- Personal data (of staff, relations or members) shall not be provided to third parties.

Remote work

The following is expected of staff/volunteers/trainees:

- Staff/volunteers/trainees working remotely – using Citrix or via webmail – must ascertain that the network where they are working is secure.
- If the network is not secure, working with Citrix remotely is not allowed. They also need to be aware of their surroundings (can anybody be watching?)
- If documents need to be downloaded on computers or sent by email, this is permitted only, if they do not contain personal data.
- Regarding the use of personal laptops, I-pads, usb sticks, mobile phones or other digital data carriers, these need to be switched off or locked, when users are no longer working remotely, so that they cannot be hacked.
- Personal data may not be gathered or retained, if cloud data storage applications are used (Dropbox, google docs etc.). Such information may be added, processed and retained only in a secure environment on the HuC servers where the KNHG has disk space.

- No documents containing privacy-sensitive info (such as for example lists of participants, mails with info from members etc.) may be left lying about in places where people work remotely.

Data leaks

If a data leak is noted within the KNHG, the staff/volunteers/trainees concerned will report this immediately to the KNHG director, who will notify the chair of the board and the Dutch Data Protection Authority without delay. All necessary (technical) steps to seal the data leak will be taken immediately as well.

Signature

Staff employed by the KNHG shall receive two copies of this protocol and shall sign it no later than 25 May 2018. Upon entering their traineeship or service, KNHG volunteers/trainees are given two copies of this protocol. On their first day at work they shall return a signed copy to the KNHG director, who shall retain these documents in a separate folder in a locked place at the KNHG office.

Updating

This protocol was drafted on 8 May 2018 and updated on 23 May.

I …….. hereby confirm that on …… I received, understood and signed this protocol for approval.