** AVG Awareness and Risk Management Plan ENMC**

**General Data Protection Regulation** (**GDPR**)

Baarn, 8 March 2018,

GDPR (Regulation (EU) 2016/6791) is a regulation by which the European Commission intends to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the data protection directive (officially Directive 95/46/EC) of 1995. This new regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require national governments to pass any enabling legislation, and is thus directly binding and applicable. In Dutch, the GDPR is called Algemene Verordening Gegevensbescherming (AVG), the ENMC is under Dutch Law and adheres therefore to the AVG.

**Is the AVG applicable to the ENMC**?

The AVG is applicable for all organisations which store and process personal data. Whether you are a large or small organization or freelancer. Commercial or non-profit organization . The Personal Data Authority (PDA), which will perform AVG inspections, are entitled to fine non-compliant organisations to a maximum of 20 million euro or 4% of the worldwide profit.

At different levels in the organization, the ENMC collects, saves, revises and uses personal data of different individuals:

1. **Candidates on the participants list of workshop applications**. Their contact details are collected and stored in the CRM system, Perfect View (PV). The office uses this database to invite participants for a new workshop, to communicate with the participants about the logistics of the upcoming workshop and to disseminate the workshop publications after the workshop.
2. **Subscribers to the ENMC newsletter in Mail Chimp**. The e-mail addresses of the subscribers are saved on the Newsletter Send List within the online system of Mail Chimp. Every half year that a newsletter is being sent by the office via Mail Chimp, this list is activated.
3. **Website visitors**. If someone is submitting personal data via the contact page, the ENMC receives the visitor’s personal information via e-mail and stores it automatically in Outlook, or if requested by the individual in PV.
4. **Personal data of employees**. In the first three examples, only contact data are being saved and processed. In the case of ENMC employees and external consultants/bureaus, also higher sensitive information (financial, national insurance number, pictures etc.) is stored and visible within the administrative systems of the ENMC and the external salary administration of NBC accountants.

The ENMC is entitled to collect, save, revise and use personal data of all four groups, since the ENMC either has received permission to use the personal data by the individuals and/or the ENMC has a legal contract with the individual. However, the ENMC needs to be able to demonstrate that these permissions have been (and will be) obtained according to AVG. Therefore, ENMC has implemented several steps and procedures to safeguard the personal data that the ENMC collects.

**What did the ENMC implement to be compliant with the AVG?**

The ENMC is entitled to collect, save, revise and use personal data of all four groups, since the ENMC either has received permission to use the personal data by the individuals and/or the ENMC has a legal contract with the individual. However, the ENMC needs to be able to demonstrate that these permissions have been (and will be) obtained according to AVG. Therefore, ENMC has implemented several steps and procedures to safeguard the personal data that the ENMC collects. It starts with creating awareness within the ENMC organization and within the group of external consultants and bureaus the ENMC is working with. The latter process has been started since January 2018. On April 19th, the ENMC Executive Committee will be informed on the AVG and its consequences for the ENMC. All members of the ENMC network will be notified by mail about the way the ENMC is following the AVG and hence is able to guarantee the safety of their personal data.

**The aims identified for which the ENMC is using personal data are:**

1: to invite for and communicate with participants for ENMC workshops.

2: to provide a contact list to all workshop participants for use after the workshop if a consortium or working group has been formed.

2: to inform the ENMC network with newsletters, year program, leaflets, availability of lay reports and publications resulting from the workshops.

3: to run a professional organisation with employees and external consultants, who are either on the payroll of the ENMC or have a project contract with the ENMC.

**Rights of the individuals**

Individuals have the right to:

* get insight in the data being stored and used by the ENMC
* change their data at any time
* delete their data at any given time point
* transfer their data outside the ENMC organization (this means that they should easily have access to their data and be able to transfer it to another organization if they want to)
* receive information about what happens with their data, when, by whom and for how long their data is being stored
* complain with the PDA in case they feel ENMC is not correctly handling their personal data.

**Kind of data being stored in the ENMC CRM system Perfect View:**

1. First name

2. Surname

3. E-mail

4. Telephone number

5. Institute

6. Address of the institute

7. Discipline (basic, clinical, translational, etc.)

8. Country

9. Salutation, Dr. or Prof.

**Accuracy by the ENMC**

The ENMC does not require an official **Data Protection Officer**, since the ENMC:

* is not a governmental institute/organisation,
* does not process highly sensitive, judicial and/or confidential data on a large scale,
* is not observing the individuals on a regular basis

However, the Managing Director of the ENMC in consultation with an independent AVG expert, is responsible for monitoring the AVG compliance of the ENMC and its measures taken, on a regular basis.

To strive for accuracy, the following precautions were made to think ahead about risks and the necessary tools to prevent these risks:

1. Implementation of a **Data Protection Impact assessment (DPIA)**, to anticipate on possible data leaking risks and describe the technical measures ENMC should take in case of privacy risk (e.g. mails containing personal data accidently sent to the wrong recipient).
	1. Measures: determine the extent of harm this accident may cause the individual who’s personal data were leaking to the wrong recipient.
	2. make sure the recipient is being notified and that the personal data can no longer be viewed/used.
	3. Notify the individual who’s personal data were sent to the wrong recipient.

This kind of Case Awareness and Corrective Actions (CAPA’s) are ongoing collected in an Excel sheet, available at the P-server in the ENMC in Baarn and form the basis for the ENMC personnel to take action in case of a data protection breach**.**

1. Incorporation of **Privacy by Design**, which means that ENMC takes care in all communication that personal data are protected (e.g. e-mails in BCC) and it describes which data minimally are required for fulfilling the goals (need-to have data) and that ENMC will not store these data longer than necessary.
2. Incorporation of **Privacy by Default**, which means that ENMC executes technical measures to ensure that only need-to-have data are collected and no longer stored than necessary (e.g. if someone has indicated to step out of the ENMC network)

**Obligations of the ENMC**

With the effectuation of the GDPR law, ENMC is held accountable for all personal data stored and used within its systems. The ENMC must be able to demonstrate that correct organizational and technical measures have been taken to comply with the GDPR. In addition, ENMC must be able to prove that valid permission by each individual has been given to process her/his personal data.

***ENMC organizational measures:***

* Set up of a **Register of Processing Operations (RPO)**, documenting which personal data the ENMC collects and processes for what aim, and by whom. What the source is of the data and with whom the ENMC shares the data.
* Employees and external consultants who have insight in the personal data stored have signed a **Confidentiality Agreement**.
* Employees and external consultants who process these data are explicitly mentioned in the Register of Processing Operations (RPO).
* External consultants and bureaus have provided the ENMC with their own signed **Data Processor Agreements** **(DPAs),** such as NBC consultant, Perfect View, CWTS and Anymazed etc.
* Procedure for **Data Leaking (DL)** has been set up already last year, but required revision because the AVG has stricter rules compared with the former Law on Data Protection (compulsory registration of all data leaks, also the ones caused by external consultants and bureaus).

***ENMC technical measures:***

* Increased Outlook2 fire-wall under auspices of Spierziekten Netherlands.
* Perfect View Cloud application3 has its own technical measures to prevent data leaking
* ENMC has a Privacy Policy published on its website4, which describes the rights of website visitors and obligations of the ENMC organisation to protect personal data of people who subscribe to our newsletter, contact ENMC to inquire for information about workshops, guidelines for application, etc. On the basis of this Policy, people may choose further access to the ENMC website.
* Mail Chimp5 has a Privacy Policy in place which secures the accessibility to the list of ENMC subscriber e-mail addresses.

***ENMC retrieving valid permission:***

1. For candidate workshop participants, two steps have been introduced:
* The application guidelines (published on the ENMC website) state that the main workshop organiser should ask participants permission for using their personal data in the future by the ENMC. The organiser then sends an e-mail to the ENMC office with the list of participants, including the e-mail addresses and a statement that all individuals on that list have given permission to use their e-mail address for future workshop invitation and communication. The participants have been informed about the aims for capturing their personal data, their rights and the organizational and technical measures that the ENMC has undertaken to secure the protection of the collected personal data.
* At the beginning of each workshop, a list with contact details will be sent around and the ENMC staff will request all participants to check their personal data, to tick the box if they agree that the ENMC will store these data and provide the participants with all relevant information about the way ENMC is taking precautions to safeguard their data and to acknowledge the rights of the participants to get insight, to change, to delete and to transport their personal data.

2. Subscribers to ENMC newsletter have given permission to be added to the Newsletter distribution list, once they have sent the request via the ENMC website. At any time, they can unsubscribe from this list, which is immediately implemented by the Mail Chimp application.

3. In case that individuals share their personal data via the ENMC website, they give permission that data are stored, used and revised by the ENMC, the moment they sign in. The ENMC has published a Privacy Policy on its website to cover permission for website visitors.

4. Permission from employees and from external consultants/bureaus to store and use their personal data for processing monthly salaries, paying invoices and registering sick leave is provided within the legal contract agreed upon by both parties.

1 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>

2 <http://spierziekten> Nederland; Firewall Outlook

3 <https://www.perfectviewcrm.nl/over-ons/veiligheid/>

4 [www.enmc.org](http://www.enmc.org)

5 <https://mailchimp.com/legal/privacy/>