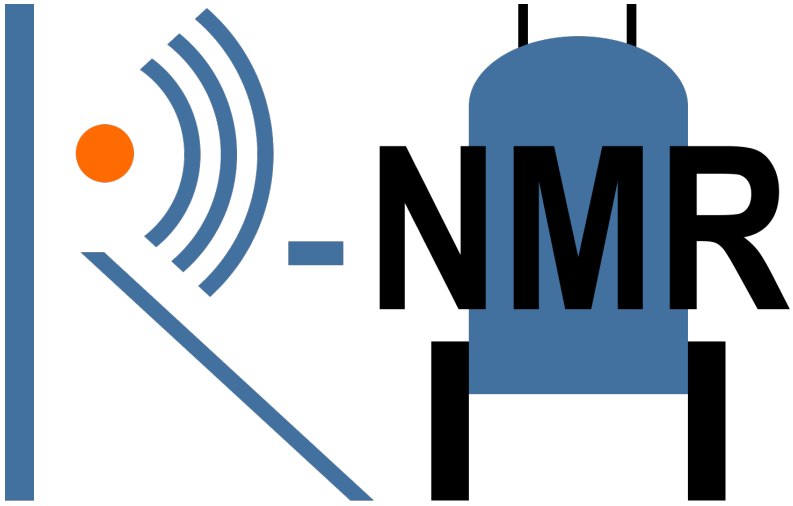

Fact Sheet and Guidelines on GDPR as it relates to NMR Facilities

of Remote NMR (R-NMR):

Moving NMR infrastructures to remote access capabilities

Authors: Göran Karlsson *(UGOT), Anders Bay Nord (UGOT) and Christina Redfield (UOXF)*

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement N. 101058595

What is GDPR?

GDPR is a regulation in EU law that governs data protection and privacy. It is essential that defining a common procedure for remote access to NMR spectrometers meets GDPR requirements with respect to the data that is collected and stored at each NMR facility, and how that data is shared with users. GDPR applies to the processing of personal data. Personal data is any information that refers to an identified or identifiable natural person. What is crucial is that the information on its own or in combination with other information can be linked to a living person. Typical personal data includes:

- a person's personal identity number,
- name,
- address,
- email address.

In the context of NMR facilities, personal data collected/stored is likely to refer to users of the NMR facility. GDPR stipulates that a person can request to be informed about their registered data and to have their registered personal data deleted.

Certain personal data is by its nature particularly **sensitive** and therefore has stronger protection. This type of data is called *sensitive personal data*. Processing of sensitive personal data is as a rule prohibited but there are certain exceptions. Sensitive personal data is data concerning:

- ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- membership of a trade union,
- health,
- a person's sex life or sexual orientation,
- genetic data,
- biometric data that is being used to uniquely identify a person.

From an NMR perspective, analysis of human biomaterial (biofluids, tissue, extracts from tissue, *etc*.) can generate information, for example, on health or drug abuse, that is considered to be sensitive personal data, if that data can be traced to a person. It is important to note that a coded sample can still be traced through a pseudo-anonymized coding list. Only truly anonymized samples, which cannot be traced to a person, are not subject to the GDPR.

Guidelines

1) Personal data collected/stored at NMR Facilities

Most NMR facilities keep a register of their users in some form (list of users' names/email addresses, LIMS/electronic notebook, Excel spreadsheet, *etc*). NMR facilities must be able to provide all information about a user if requested to do so by that user and to delete that personal data upon request by that user. Personal data relating to NMR users is similar to the information kept by department/university IT services about users of their IT facilities. It is the overarching responsibility of the universities and specifically university administrations, or other legal entities, hosting the NMR facilities to have procedures in place relating to GPDR and the handling of personal data. This is the ultimate source from which proper guidelines and information on operating procedures under the GDPR must be obtained. This should not have to be re-invented at the NMR facility level.

2) Sensitive personal data collected/stored at NMR Facilities

From an NMR Facility perspective, metabolomic studies involving human biomaterial are the most likely source of sensitive personal data (if that data can be traced to a person). It is important to note that a coded sample can usually still be traced through a pseudo-anonymized coding list. The data are considered sensitive even if the pseudo-anonymized coding list is not available at the NMR Facility. Only truly anonymized samples, which cannot be traced to a person, are not subject to the GDPR. NMR studies involving human biomaterials will normally have been granted ethical approval via an appropriate institutional committee and the NMR Facility should confirm that such approval is in place.

If the NMR Facility is involved in the collection or processing of sensitive personal data, then this must comply with a number of requirements imposed by GDPR. These are:

- Data and meta-data (during the statistical analysis of metabolomics data) should be F.A.I.R. (Findable, Accessible, Interoperable, Reusable) and minimal.
- The sending/receiving of meta-data should be secure (*e.g.* not via regular e-mail).
- Acquired data should not be left on spectrometer hard drives for general access.
- Access to stored data should be secure (*e.g.* MFA, multi-factor authorization) and traceable.
- Analysis of data should be in a secure environment (*e.g.* using MFA, access events should be logged).
- Transfer of data should follow the same principles (e.g. MFS, secure, logged, traceable).
- Data and meta-data should routinely be deleted after a fixed period of time unless permission is obtained to keep the data for an extended period.

When carrying out NMR studies involving sensitive personal data, NMR Facilities must ensure that the acquisition of NMR data, the storage of acquired NMR data, the analysis of stored

NMR data, the handling of meta-data, and the transfer of stored NMR data (including meta-data, analysis results, *etc*) comply with the above GDPR requirements.

The NMR Facility must be able to identify the personal data controller and the personal data processor. The data controller is defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The data processor is defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. The personal data controller or processor do not need to be individuals working within the NMR Facility but the Facility Manager must know who they are within the institution.

Again, it is the overarching responsibility of the universities and specifically university administrations, or other legal entities, hosting the NMR facilities to have procedures in place relating to GPDR and the handling of sensitive personal data. This is the ultimate source from which proper guidelines and information on operating procedures under the GDPR must be obtained. This should not have to be re-invented at the NMR facility level.