GDPR compliance in DHIS2 with regard to the COVID-19 packages.

This document describes the current status of GDPR compliance within the DHIS2 system configured for use of COVID-19 tracking with one of the COVID-19 packages from WHO. Since DHIS2 is a highly configurable system when it comes to what kind of data is collected and how it is processed this document will describe how GDPR compliance is met within the boundaries of a standard DHIS2 system configured with COVID-19 metadata packages only.

(Art. 5 GDPR – Principles relating to processing of personal data)

https://gdpr-info.eu/art-5-gdpr/

A. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

a. The DHIS2 server, clients and the COVID-19 packages are 100% open-source (BSD-3) https://github.com/dhis2/dhis2-core/blob/master/LICENSE, and designed to be downloaded and hosted on the implementers own servers. The implementing party has, therefore, the highest available transparency regarding insight into how the system operates.
How the data is used after collection is outside control of DHIS2, however, DHIS2 default system configuration and recommended collection and processing practices are always carefully designed to follow sound ethical norms and guidelines.

B. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

a. The COVID-19 packages are constructed in partnership by WHO and are designed to only collect data relevant to COVID-19 tracking.

b. The consent documents used by the respective implementing party before collecting data is outside the scope of the DHIS2 system.

c. The data retention policy is up to the implementing party to decide and highly specific to local laws. The DHIS2 has the needed functionality to completely delete the records when requested.

C. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

a. The specific data collected for the COVID-19 tracking application is described in the COVID-19 metadata package documentation.

D. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

a. The COVID-19 packages are quality controlled and tested by WHO, the DHIS2 organization and all the implementing countries. The DHIS2 system has an advanced graphical user interface which helps the data collector to collect the correct information and gives guidelines on how to correct data that is for example wrongfully entered, e.g a number in a name field.
There are training programs and online resources available in multiple languages for the implementers to use and adapt for setting set up for example local training schools/academies.

b. The ability for the “patient” to request deletion and ratification is highly dependent on the local laws and the implementing party, like how they choose to set up the processes and infrastructure to handle such requests. The technical functionality in DHIS2 is supportive to accommodate this, i.e. 100% erase and rectify records.

E. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

a. This is 100% controlled by the implementing party. DHIS2 has the needed functionally to query data on for example created date or person id and the ability to delete all the “patients” data from the database.

b. Absolutely no data collected or generated is sent to any external server out of reach/access to the implementers.

F. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

a. DHIS2 has state-of-the-art access control and can limit access to data based on many parameters. Access can be limited to the relevant implementing parties predefined user groups in several ways. DHIS2 supports two-factor authentication and has gone through several security audits and penetration tests from external independent organizations.

b. DHIS2 supports encryption of sensitive/confidential attributes.

c. The data layer in DHIS2 has extensive data audit functionality to log all data entries, modifications and lookups.

Process

GDPR implies a software development process which incorporates principles of security by design. DHIS2 is a dynamic artefact which is daily being designed, produced, used, redesigned and reproduced in a constant cycle. To ensure security management of the process we have instigated the following measures:

I. we have a multi-disciplinary security team which responds within 24 hours to critical vulnerability reports from the field and other sources such as penetration tests;
II. we have a dedicated security engineer;
III. we have a vulnerability management system where vulnerabilities are given treatment which is different to other reported issues;
IV. we have a vulnerability disclosure program for trusted partners, which will get access to critical security issues before they are publicly disclosed.

As a university with Scandinavian action research tradition, we also have a stream of masters research into a very wide range of security related topics which feed back into the development process, including : pentesting, web application firewalls, information security management and ASVS process.

The Case of Norway

The DHIS2 COVID-19 tracking system is the first implementation and use of DHIS2 in Norway. To date (28/07/2020), 44 municipalities are using it for contact tracing and case surveillance. The instances are centrally managed in a national server hosting facility operated by the National Association of Local and Regional Authorities (KS in Norwegian). Before starting this

process and in order to comply with Norwegian regulations, each municipality and KS had to perform a risk assessment which included GDPR compliance of the implementation as well as Norwegian regulations related to patient confidentiality. Their conclusion was that DHIS2 was capable of complying with GDPR requirements.