


| | | | |
|--|-------------------------|---------------------|---|
| GenomeScan Data Security Policy (Annex 1) | | |  |
| Short Name: DSP Annex 1 | | | |
| File name: Data Policy GSCAN (annex 1) | | | |
| Version: addendum 2020 | Date: 2020-08-18 | Page: 1 of 1 | Editor: n.a. |

Annex 1: Privacy Statement

GenomeScan takes the view that the confidentiality of all personal data that has been provided to the company directly by the data subjects or indirectly via other organizations should always be respected. In processing such personal data GenomeScan acts in accordance with the EU General Data Protection Regulation (GDPR) and its internal Data Security Policy. The GenomeScan Data Security Policy Is embedded in the companies' Quality Management System (QMS). The system is demonstrably compliant with the International standards ISO/IEC 17025 and ISO 15189. Furthermore, it is our policy to work in full compliance with NEN 7510 and NEN 7512.

Genetic information is generally regarded as sensitive personal data. GenomeScan therefore prefers to work with fully pseudonymized data and strives to minimize the number of independent data items it stores per data subject. GenomeScan will only process personal data if this is permitted by law. GenomeScan will restrict data processing to activities directly related to the purpose as specified in the informed consent and/or the Data Processing Agreement. GenomeScan will not share any data with third parties, including subcontractors, unless this has been agreed with the data subject or his/her representative.

Both electronic and physical access to our computer systems are strictly controlled. All employees are well-trained and legally bound to confidentiality rules. Sequence data is encrypted after analysis and safely retained for 20 years, unless a shorter retention time has been agreed with the customer. Meta data is securely stored for 20 years and back-ups are made on a regular basis. After the retention time, both data and back-ups are destroyed. When personal data must be transferred, GenomeScan will encrypt the data before shipment. An incident response plan has been defined to ensure effective and orderly response to incidents (possibly) involving personal data.

Under GDPR, data subjects (e.g. patients) have specific rights. Usually these rights are: The right to be informed, the right of access (not always free of charge), the right of rectification, the right to be forgotten (or anonymized), the right to restrict processing, the right to data portability, and the right to object to processing.

If a data subject has a request related to his/her rights, he/she should send the request together with a proof of his/her identity to our Data Protection Officer (email: DPO@genomescan.nl). If anyone has a question or complaint about our data processing, he/she can contact the Data Protection Officer. If needed, a complaint can be lodged with the supervisory authority, the Dutch Data Protection Authority ('Autoriteit Persoonsgegevens').