PROTECTION OF PERSONAL DATA

GRI Standards :

418-1 : Customer privacy

EXECUTIVE SUMMARY

"Personal data" refers to any information that can be used to identify an individual, whether directly (e.g. name, date of birth, social security number, etc.) or indirectly (e.g. bank account number, network ID, etc.). Sanofi's activities require, by nature, the use of personal data which may be sensitive, such as data related to health. Hence, Sanofi is committed to taking appropriate and responsible measures to protect the privacy and the personal data of its employees and its stakeholders (patients, health care professionals, etc.).

As Sanofi operates across all international markets, we have issued stringent harmonized Group Personal Data Protection rules applicable to all our employees throughout the world, which facilitates the transfers, process and data governance within the group in compliance with countries' legislations, such as the General Data Protection Regulation (the "GDPR") in Europe since 25 May 2018 or the California Consumer Protection Act (the "CCPA") which came into force on 1 January 2020. Sanofi's processing of personal data relies on internal and external policies, which are publicly available on the global corporate website and entitles the collection, use, disclosure, transfer, storage and other Processing of Personal Data worldwide.

TABLE OF CONTENTS

1. BACKGROUND

Sanofi is committed to handling Personal Data responsibly in order to earn and preserve the trust of any third party interacting with the Group and to prevent the Group from inappropriate personal data management process.

Data protection and privacy legislation varies from country to country. In Europe, the General Data Protection Regulation (the "**GDPR**") came into force on 25 May 2018 and has harmonized significantly (although not fully) EU national data protection laws. This legislation has significantly increased the level of expectations for companies processing personal data, notably through the imposition of a new principle of "accountability" which requires that any company processing personal data is able to demonstrate, at all times, that it complies with the requirements of the GDPR, notably by documenting the manner in which personal data is processed.

"Personal data" means any information that can be used to identify an individual, whether directly or indirectly (e.g. name, date of birth, social security number, photograph, e-mail address, computer ID).

The scope of personal data is very wide. It includes directly identifying information such as name, picture, social security number, etc. It also includes indirectly identifying information, such as bank account number, network ID, etc.).

"Personal data processing" means any operation or set of operations performed upon personal data, whatever method is used. In other words, any use of personal data should be considered as a personal data processing. A personal data processing can be computerized (e.g. video surveillance, files transfers over the Internet, electronic databases, etc.) or manual (e.g. paper files).

Because Sanofi operates across all international markets, we have issued stringent harmonized Group Personal Data Protection rules applicable to all our employees throughout the world.

To facilitate transfers of data within the Group, we have adopted "Binding Corporate Rules", which govern the manner in which personal data is processed by entities of the Group located outside the European Union when receiving certain personal data transfers from a European subsidiary.

2. ORGANIZATION AND POLICIES

Sanofi's activities require, by nature, the implementation of numerous processes involving personal data. The use of such data may involve sensitive personal data (for instance data relating to health)...

This is why Sanofi is committed to taking appropriate measures to protect the privacy and the personal data of its employees and of third parties with whom Sanofi interacts (patients enrolled in clinical trials, healthcare professionals, contractors, scientists, etc.).

For this purpose, Sanofi has adopted several standards and procedures defining the principles and measures which have to be respected and implemented when processing personal data.

2.1. Sanofi Group Data Protection Office

Since May 2013, Sanofi has had in its organization a Privacy and Data Protection Function, chaired by the Group Data Protection Officer. In 2019, a new Group Data Protection Officer has been appointed and is responsible for ensuring the implementation of a Corporate Privacy and Personal

Data Protection programs within the Group. The role of the DPO is to reinforce all actions to enhance a culture of respect for the privacy of patients, employees, and business partners worldwide.

To achieve this goal, Sanofi's Group Data Protection Officer relies on a corporate privacy team (the Global Privacy Office) and on an International Privacy Officers Network of Local Privacy Officers ("**LPOs**") established in countries where Sanofi's affiliates are established.

It also relies on a network of Functional Privacy Officers ("**FPOs**") representing Global Functions such as Research & Development, Human Resources, Information Technology & Solutions, Finance, Business Services, Industrial Affairs, as well as the Global Business Units.

In 2019 a new tool, OneTrust has been rolled out by the Global Privacy Office, for use by any Sanofi employee needing to process personal data. The tool allows to assess the compliance of the project with regards to personal data protection regulations and Sanofi policy; define corrective actions to be implemented; maintain up to date the registry of data processing of the Sanofi group and thereby ensure the traceability of projects implying personal data processing.

For more information: Contact the Global Privacy Office at Privacy-Office-Global@sanofi.com

2.2. Standards

The description of Sanofi's approach to the processing of personal data is set out in two documents, the Sanofi Global External Privacy and Data Protection Policy and the Sanofi Global Internal Privacy Standard.

The External Policy, which is publicly available on Sanofi's global corporate website, provides a general description of Sanofi's processes involving the data of third parties (patients, healthcare professionals, etc.) by explaining the purposes of processing, the categories of data processed and other details.

For more information:

https://www.sanofi.com/en/our-responsibility/sanofi-global-privacy-policy

The Internal Standard defines the main principles applicable to the processing of personal data by any Sanofi entity with a view to guarantee every individual's right to privacy in accordance with the GDPR. It defines high-level standards as a minimum requirement in order to ensure an adequate level of protection within Sanofi for the collection, use, disclosure, transfer, storage and other Processing of Personal Data.

The two standards are global in scope and apply to Sanofi around the world and to all Sanofi employee processing personal data. The commitments and obligations set out in these Standards are without prejudice to the application of and compliance with the privacy laws and/or culture of each country in which Sanofi operates when processing personal data anywhere in Sanofi. As a result, while processing personal data, all Sanofi entities and Sanofi employees must also consider local legislation and comply with applicable legal or regulatory provisions governing such processing of data in their respective country.

The requirements defined in the Internal Standard are also applicable to third parties processing personal data on behalf of Sanofi, such as consultants, service providers, vendors or other partners, for instance by way of contractual provisions.

This Internal Standard concerns all Personal Data Sanofi is processing and applies:

- To any individual's Personal Data regardless of citizenship, whether, in particular, a Sanofi employee or a member of his/her family, an applicant for a position, a patient, customer or

healthcare professional, a party to an agreement with Sanofi such as a supplier, or subcontractor, or any visitors, etc.;

- For any kind of Personal Data Processing regardless of the medium used (electronic, paper, other) and purpose, namely, without limitation: personnel files, supplier management files as well as those relating to the management of parties to agreements with Sanofi, files which have a direct connection with Sanofi's activity, such as clinical trial monitoring, pharmacovigilance, customer files, etc.

2.3. Code of Ethics

In support to the efficiency and binding nature of Sanofi's Global Privacy and Personal Data Protection Standards, Sanofi's Code of Ethics contains a chapter that addresses respect for private life and personal data protection.

In this document, which is available to all employees and to third parties working with the Group, Sanofi confirms its commitment to protecting personal data by guaranteeing a person's right to exercise control over the collection, processing, use, disclosure, and storage of personal data relating to them.

Under the Code of Ethics, Sanofi employees must comply with all international and national laws and regulations governing the management of personal data.

All our employees, and third parties with whom Sanofi has dealings (patients enrolled in clinical trials, medical practitioners, contractors, representatives of the scientific community, etc.), are entitled to their privacy.

Global Privacy Office has also published an Employee Privacy Notice – available on GPO intranet - that describes the general practices of the Group in respect of the processing of Employee's Personal Data, and in particular the different type of purposes for which SANOFI may process their Personal Data.

For more information, see in our Document Center :

> *Sanofi Code of Ethics*

> *Ethics in Business factsheet*

2.4. Processing of Personal Data of patients involved in clinical trials and monitoring of pharmacovigilance information

The very nature of Sanofi's activity requires the processing of data of individuals who receive our treatments (collected in clinical trials, genetic and epidemiological studies, during the monitoring of pharmacovigilance information or within the frame of Patient Support Programs).

Patients' Personal Data collected in clinical trials may include: age, gender, medical history, phenotype (set of observable characteristics such as anatomy, morphology), genotype (gene composition), and so on.

At Sanofi, informed consent is required each time a patient participates in a clinical trial. Informed consent ensures respect for both voluntary participation in the study and for the patient's right to privacy and data protection consistent with the requirements of applicable law. No consent is required for the reporting of adverse events in the course of pharmacovigilance, but the person who reports the case, most often the healthcare professional, will inform the patient of the transfer of non-directly identifiable health data relating to him or her. This transfer is restricted to pharmacovigilance

purposes and to the market-authorization holder and health authorities in charge of pharmacovigilance.

Sanofi's approach regarding the processing of these categories of personal data is based on the Code of Ethics and the Group's Global Privacy Standard.

2.5. Sanofi's Binding Corporate Rules (BCRs)

In line with the rules which existed previously, under GDPR, transfers of personal data from a European Union country to a non-EU country are regulated. Indeed, personal data must be adequately protected when transferred outside of the EU since non-EU countries' regulations do not always ensure a sufficient level of personal data protection.

To facilitate personal data flows within the Group, Sanofi has adopted a set of Binding Corporate Rules (BCRs). BCRs are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection.

Sanofi's BCRS have been validated by the French national data protection authority (CNIL) and by each authority in charge of personal data protection within EU member states in which Sanofi operates in 2009. Outside the EU, each Sanofi affiliate has signed a contract, making explicit their commitment to respect these rules.

The Binding Corporate Rules are currently under substantial review by Global Privacy Office to ensure that :

- it is compliant with the new rules set forth by the GDPR in 2018;
- it reflect the new governance framework implemented since 2018 by Global Privacy Office;
- it covers a wider typology of transfers and processing activities.

For more information, see in our Document Center: Binding corporate rules document.

3. ACTION PLAN

3.1. Developing awareness in-house and implementing training tools

Sanofi has developed and published a series of 12 awareness videos that cover key-aspects of Data Protection rules within SANOFI ("*Privacy@SANOFI : let's puzzle it out*"). The series is available on the Global Privacy Office's intranet site, and has been distributed in various countries through the International Privacy Officers' Network. It covers :

- The basics of Data Protection (what is personal data etc.);
- How to ensure transparency with Data Subjects;
- How to safeguard transfers of Personal Data through adequate contracts;
- How to implement Privacy-By-Design within a Project;
- How to assess the risks through ONETRUST and the completion of a PDPA;
- How to report a Data Breach;

- How to handle Data Subject Access requests;
- How to ensure that vendors offers sufficient Data Protection warranties.

On the basis of this series, Global Privacy Office is currently redesigning the iLearn training offer to ensure that the key-topics above are implemented in mandatory training modules. These new modules are expected to be released at the end of Q2.

In addition to the above:

- Live-training sessions have been rolled out throughout the world by the network of Privacy Officers on various topic (such as “how to carry out a PDPA” or “how to ensure vendors offers sufficient Data Protection warranties”);
- An interactive guidance document (“My Privacy Checklist”) has been published to raise awareness on the key-aspects of Privacy and how such principles apply in practice at SANOFI;
- A full 13-hour training curriculum on privacy and data protection, primarily aimed at the LPOs and FPOs to help them carry out their roles but available to all interested employees
- A module designed for Research & Development activities, focusing specifically on clinical trials and pharmacovigilance is also under review, in parallel to the redesign of the Study Compliance Form process.