CDISC Policy

Data Protection

Revision History

Date	Revision	Description	Author
December 2018	1	Original Draft	CDISC Legal Advisors
May 2019	1	Approval	Board of Directors

DATA PROTECTION POLICY

1. PURPOSE OF THIS POLICY

1.1. As an international non-profit organisation working to develop clinical data standards of the highest quality, CDISC takes great care to protect the personal data and privacy of individuals.

1.2. For CDISC, it is never acceptable that personal data is handled in a way which is unlawful or which could cause distress or damage to the individuals to which the data relates (**Individuals**) or put their safety or wellbeing at risk.

1.3. The privacy and rights of all Individuals with whom CDISC engages is of paramount importance to us. CDISC is committed to safeguarding their privacy by handling personal data in accordance with the data protection and privacy laws which apply to CDISC (**Data Protection Laws**). This includes state and federal privacy laws and, where applicable, the General Data Protection Regulation (**GDPR**) (please see section 4 for further details on when the GDPR applies to CDISC).

2. WHO THIS POLICY APPLIES TO

This Data Protection Policy applies to all CDISC directors, officers, members, employees, consultants, contractors, temporary and agency workers and other staff (**CDISC Staff**). CDISC Staff must read, understand and comply with this Data Protection Policy when *processing personal data* on CDISC's behalf and on behalf of CDISC's members.

3. CDISC's DATA PRIVACY COMMITTEE & WHEN TO CONTACT THEM

3.1. CDISC's compliance with Data Protection Laws is supervised by CDISC's Data Privacy Committee, which is comprised of the CEO, the COO, the IT Manager and any other member designated by the CEO from time to time.

3.2. CDISC Staff should contact a member of the Data Privacy Committee whenever they have a question about processing personal data of Individuals in the course of performing their duties or if they have any concerns that this Data Protection Policy is not being or has not been followed.

4. ABOUT THE GDPR

4.1. The GDPR is comprehensive data protection law which was introduced in May 2018 by the European Union. It has extra-territorial effect and can apply to organisations or persons anywhere in the world which processes personal data (including CDISC).

4.2. CDISC may not be directly regulated as a controller under GDPR, it is still committed to fostering a culture of data protection throughout the organisation by complying strictly with Data Protection Laws both for its own regulatory compliance purposes and also for the benefit of its members. As a result, the standards for handling personal data set out in this Data Protection Policy are intended to meet the stringent new standards established by the GDPR.

5. THE IMPORTANCE OF DATA PROTECTION COMPLIANCE TO CDISC

5.1. Any breaches of Data Protection Laws by CDISC could have very serious consequences for Individuals and for the organization, including:

(i) Individuals could suffer emotional distress, financial damage or even have their safety put at risk.

(ii) CDISC could be subject to investigations, which would likely result in reputational damage and adverse media scrutiny.

(iii) CDISC could have fines imposed (the GDPR provides for fines of up to EUR 20 million (approx. USD $22.5 million)) and may even have parts of business operations suspended or stopped.

(iv) It could cause members to lose trust in the organization, which in would negatively impact CDISC work.

(v) It could result in members terminating their membership with CDISC and bringing claims for compensation arising from any damage they have suffered as a result (which could be significant).

5.2. Given the risks of not handling personal data in accordance with this Data Protection Policy, CDISC Staff non-compliance may:

(i) If they are an employee, result in disciplinary action, up to and including dismissal.

(ii) If they are a contractor, consultant or agency worker, result in the review, non-renewal or termination of the contract governing their provision of services to CDISC and potentially even claims for compensation against them or their employing organisation.

5.3. In some cases (such as intentionally mishandling personal data, or data theft), a breach of Data Protection Laws can be a criminal offence, and can result in a criminal record, fine and even a prison sentence for CDISC Staff who have mishandled the data.

6. PROTECTION OF PERSONAL DATA: A FUNDAMENTAL RIGHT

6.1. This Data Protection Policy is built around the data protection principles contained within the GDPR. These principles reflect the view that the protection of personal data is a fundamental right for Individuals.

6.2. The GDPR provides an extensive legal regime for protecting the personal data of Individuals by:

(i) Imposing broad obligations on organisations such as CDISC which collect personal data and have control over how and why personal data are processed (these are known as **data controllers**).

(ii) Imposing obligations on organisations that process personal data on behalf of a data controller (these are known as **data processors**).

(iii) Conferring broad rights on Individuals about whom data are collected (these are known as **data subjects**).

7. KEY CONCEPTS

7.1. There are several key concepts which it is important for CDISC Staff to be aware of in order to understand this Data Protection Policy and to be able to act in accordance with it:

Personal data

7.2. This is defined broadly to mean any information which can be used to identify an individual, taking into account various factors such as those specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

7.3. Typical examples of personal data processed by CDISC include:

(i) Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.

(ii) Social security numbers, bank account details, payroll records and tax status information.

(iii) Salary, annual leave, pension and benefits information.

(iv) Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process.

(v) Employment records, including job titles, work history, working hours, training records and professional memberships.

(vi) Date of birth, gender, marital status and dependants.

(vii) Compensation history and performance information.

(viii) Information about employee health, including medical conditions, health and sickness records.

(ix) Personal data which CDISC processes on behalf of others.

Sensitive personal data

7.4. The GPDR imposes additional obligations in relation to certain types of so-called special categories of "sensitive" data, which include any personal data which reveal or relate to an Individual's: (a) racial or ethnic origin; (b) political opinions; (c) religious or philosophical beliefs; (d) trade union membership; (e) genetic data; (f) biometric data; (g) health; (h) sex life or sexual orientation.

7.5. Some of these categories of sensitive information are unlikely to apply to data held by CDISC. However, others will be. For example, as an employer CDISC may hold sensitive personal data about employees (such as health data relating to illness and absences, or accidents at work). CDISC might also hold details of

racial or ethnic origin about staff (for example, if this information is contained within a passport which CDISC stores a copy of for right to work or identification purposes).

Processing

7.6. This core concept is also broadly defined and covers most operations involving personal data such as collecting, recording, storing, retrieving and transmitting personal data as well as blocking, erasing or destroying it. At a day-to-day level, CDISC Staff should assume that anything which they are doing with personal data will be regulated as processing of it.

Anonymisation & Pseudonymisation

7.7. The GDPR does not apply to personal data which has been "anonymised" permanently such that the relevant Individuals can no longer be identified.

7.8. In some cases, certain information may be *temporarily* removed from personal data so that the Individual is not identifiable without that removed information, for example by using a separately stored "key" to return the data to a state which allows individuals to be identified again. This type of data is known as "pseudonymised" data and it is still regulated as personal data.

7.9. If CDISC Staff are not sure whether data is "personal data", "anonymised data" or "pseudonymised data" then they should consult a member of the Data Privacy Committee.

Accountability

7.10. CDISC must be able to demonstrate that the processing activities undertaken within CDISC comply with the data processing principles (see section 8.1 *Data Protection Principles* below). It is therefore very important that CDISC documents its compliance with Data Protection Laws by taking the following steps:

(i) Appointing the members of CDISC Data Privacy Committee to oversee CDISC compliance with Data Protection Laws and ensuring that these members remain up to date on developments relating to Data Protection Laws.

(ii) Maintaining data processing records, and organising all of CDISC data protection related documentation (such as agreements with third party processors).

(iii) Implementing Privacy by Design and by Default principles in CDISC business and undertaking Data Protection Impact Assessments where necessary.

(iv) Integrating data protection into internal documents, policies and privacy notices, and regularly training CDISC Staff on them and on relevant developments in Data Protection Laws.

(v) Regularly testing the data protection measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement efforts.

Privacy by Design and by Default

7.11. As an organisation, CDISC is required to implement appropriate technical and organisational measures to ensure that all processing of personal data in the course of its business is designed to satisfy the data protection principles (see section 8.1 *Data Protection Principles* below) and that, by default, only necessary data are processed.

Data Protection Impact Assessments

7.12. Whenever CDISC Staff engages in processing which can be considered to be "high risk", especially when using new technologies, then it is necessary to undertake a data protection impact assessment (**DPIA**). A DPIA is essentially a detailed evaluation of the potential risks posed by the proposed processing activities and determination of the appropriate measures to take to manage those risks in accordance with Data Protection Laws.

7.13. If CDISC Staff believes that any processing activities which they are considering undertaking are, or may be, high risk then they should discuss with a member of the Data Privacy Committee.

8. DATA PROTECTION PRINCIPLES

8.1. There are six key data processing principles (reflecting the data protection principles within the GDPR) which all CDISC Staff must comply with when processing personal data:

1. *Lawfulness, Fairness and Transparency*

There must be a lawful basis for collecting and processing the data in the first place. In CDISC's case, this will most often be because CDISC need to process the data for the purpose of fulfilling CDISC's contractual obligations to CDISC members, CDISC Staff and suppliers, or for other legitimate interests of CDISC.

Purpose Limitation The data must be collected only for specified, explicit and legitimate purposes, and must not be further processed in any manner incompatible with those purposes.

Data Minimisation Data must only be collected to the extent that it is adequate, relevant and necessary for the purposes for which the data is to be processed.

Accuracy The data collected must be accurate and, where necessary, kept up to date.

Storage Limitation: The data must not be kept in a form which permits the identification of Individuals for longer than is necessary for the purposes for which the data is to be processed.

Integrity and Confidentiality: The data must be processed in a manner that ensures, through appropriate technical or organisational measures, that it will be kept secure, including protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9. LAWFUL BASIS

9.1. To achieve CDISC's aim of meeting the stringent requirements of GDPR, CDISC Staff should always ensure that there is a lawful basis for using personal data.

This will be one of the following:

(1) **Consent:** Where an Individual provides his or her freely given, specific, informed consent to a particular purpose, then personal data can be used for that purpose.

(2) **Performance of a contract with an individual**: An individual's personal data can be used by us to the extent necessary to perform a contractual obligation CDISC owes to that individual (for example, under a contract of employment).

(3) **Compliance with a legal obligation:** Personal data can be used to the extent necessary to comply with a legal obligation (such as disclosing employee payroll information to the IRS).

(4) **The legitimate interests of CDISC or a third party**: Personal data can be used to the extent necessary for CDISC's legitimate interests (or those of a third party).

9.2. Personal data can also be used to the extent necessary to protect an individual's vital interests (i.e. life and death situations), or by public bodies in the exercise of official duties. However, these latter grounds are unlikely to apply to CDISC.

9.3. Additional restrictions apply to the use of sensitive personal data and data relating to criminal convictions and offences. Generally, CDISC will only be able to use such information because the individual has already made it public, or else it is with his or her consent (which must be explicit consent for sensitive data) or where necessary in connection with CDISC's rights and duties as an employer.

9.4. CDISC will attempt to find a lawful basis under GDPR for any personal data which CDISC processes and are in control of. In the event that no lawful basis can be found, but GDPR does not apply, CDISC may still process the personal data, but will make sure to protect it in accordance with this Data Protection Policy and will only use it as is necessary for a proper lawful purpose.

10. SECURITY

10.1. Whenever it processes personal data CDISC must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (in particular where the processing involves the transmission of data over a network) and against all other unlawful forms of processing.

10.2. In particular, CDISC shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate:

(i) the pseudonymisation and encryption of personal data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(iii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness

of technical and organisational measures for ensuring the security of the processing,

taking into account always the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals.

10.3. It is therefore of paramount importance that if any CDISC Staff become saware of any incidents which could put personal data at risk, or result in Individuals being subject to distress, damage or having their safety or wellbeing put at risk, they report this immediately in accordance with section 14 (Reporting) below.

11. RIGHTS OF INDIVIDUALS

11.1. The GDPR grants Individuals comprehensive, protective rights in respect of how their personal data is processed, the key rights being set out below. Where GDPR does apply to CDISC's processing activities, any requests to exercise data subject rights will be dealt with in the manner set out below. Where GDPR does not apply, CDISC's Data Privacy Committee will, in their discretion, determine if and to what extent that Individual can exercise any of the data subject rights set out in this Data Protection Policy.

11.2. Each case must be considered on its own merits and, as a general rule, CDISC will have a maximum of one month in which to respond to requests from Individuals, although this may be extended by two further months in cases which are complex or involve numerous requests.

11.3. ***If CDISC Staff receive a data subject request from an Individual, it is very important that they inform a member of the Data Privacy Committee immediately***.

11.4. **Right to be informed**: Individuals have the right to know about how their personal data will be used. CDISC must therefore be transparent about the purposes for which it uses personal data collected about Individuals. This is normally achieved by setting out the necessary information in a "privacy notice".

11.5. **Right of access:** Individuals have the right to obtain access to the personal data that CDISC holds about them, subject to certain exemptions. These requests are often referred to as "Subject Access Requests" or "SARs".

11.6. **Right to rectification**: Individuals are entitled to request that CDISC rectifies their personal data if it is inaccurate or incomplete. In certain circumstances, Individuals have the right to require that CDISC erases their personal data, for example where the data is no longer necessary, consent is withdrawn, the Individual objects to processing (and CDISC does not have a "legitimate interest" to continue it), or the data has been unlawfully processed. This is also known as the "right to be forgotten" or "RTBF".

11.7. **Right to restrict processing:** In the following circumstances, Individuals may have the right to request that the processing of their personal data is restricted:

(i) Where an Individual contests the accuracy of the personal data, CDISC should restrict the processing until CDISC has verified the accuracy of the personal data.

(ii) Where an Individual has objected to the processing (where it was necessary for the performance of a public interest task or for the purpose of legitimate interests), and CDISC is considering whether its legitimate grounds override those of the Individual.

(iii) When processing is unlawful and the Individual opposes erasure and requests restriction instead.

(iv) If CDISC no longer needs the personal data but the Individual requires the data to establish, exercise or defend a legal claim.

11.8. **Right to data portability:** Individuals have the right, in certain circumstances, to receive personal data concerning themselves from CDISC in a structured, commonly used and machine-readable format. The purpose of this right is to allow Individuals to have their personal data transferred between IT environments in a useable form. Individuals also have the right to request, where technically feasible, that the controller transmits their personal data to another controller directly.

11.9. **Right to object to processing:** Individuals have the right to object to:

(i) Direct marketing (including profiling).

(ii) Processing based on legitimate interests or the performance of a task in the public interest or exercise of official authority (including profiling).

(iii) Processing for purposes of scientific/historical research and statistics.

11.10. **Rights related to automated decision making and profiling:** Data Protection Laws provide safeguards for Individuals against the risk that a potentially damaging decision is taken without human intervention. In practice this means that Individuals have the right, subject to certain exemptions, not to be subject to a decision when:

(i) it is based on automated processing (including profiling); and

(ii) it produces a legal effect or a similarly significant effect on the Individual.

12. DATA SHARING & APPOINTING DATA PROCESSORS

12.1. As a general rule, sharing of personal data with third parties is only permitted under GDPR if undertaken in accordance with certain safeguards and if appropriate contractual arrangements have been put in place.

12.2. Generally, CDISC may only share the personal data it holds with any third party which it appoints to process personal data on CDISC's behalf (known as a "**data processor**") in a way which satisfies the stringent requirements of the GDPR and which keeps the data safe and secure.

12.3. There are a broad range of services which may be provided to us by data processors, including: (a) suppliers of IT maintenance services and hosted-software and back-up services; (b) payroll processors and benefits administrators; and (c) document destruction services (for physical documents and electronic documents).

12.4. Even though it is sometimes not immediately obvious that a supplier may be a data processor, where GDPR applies to CDISC's processing activities then CDISC is still legally responsible for all data processing undertaken by a supplier on its behalf. It is therefore very important that CDISC has full visibility as to how they will provide the processing services, and keep the data safe and secure, before entering into any contracts with them.

12.5. If any CDISC Staff is responsible for engaging with a third party supplier which will collect, store, handle or destroy personal data on CDISC's behalf then they must consult a member of the Data Privacy Committee.

13. INTERNATIONAL TRANSFERS

13.1. The GDPR imposes strict restrictions on transferring personal data to recipients in countries outside the European Economic Area ("**EEA**"). Understanding these restrictions is particularly important for CDISC Staff as CDISC may receive information from a person or organisation based in the EEA.

13.2. The general rule is that the transfer of personal data to an organisation in a country outside the EEA (**Destination Country**) is only allowed if such Destination Country has been approved by the European Commission as providing an "adequate level of protection" for the personal data. Very few countries have received such approval.[1]

13.3. Even if the Destination Country is not approved, it may be possible to transfer the data lawfully by relying on alternative methods, for example:

(i) Privacy Shield: If the recipient organisation is in the US and registered as adhering to the US-EU Privacy Shield Framework.

(ii) Model Clauses: If a data transfer agreement incorporating European Commission approved "Standard Contractual Clauses" (also known as "Model Clauses") is entered into between the organisations transferring and receiving the data.

(iii) Explicit Consent: In certain circumstances, it is possible to rely on explicit consent obtained from the relevant Individuals. This method cannot, however, be used when transferring employee data.

13.4. It is important to be aware that the concept of "transferring" personal data is very broad and is not limited to sending documents, storage devices or storage media containing personal data outside the EEA. It can also cover, for example, where CDISC Staff makes personal data which is stored on IT servers in the EEA available to individuals outside the EEA so that they can access and use such data.

13.5. The issue of international transfers should be considered not just in the context of transfers made by CDISC, but also in relation to transfers made to us (for example by members based in the EEA). In these situations, CDISC and the transferor will need to make sure one of the measures described in section 13.3 is place.

[1] The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay as offering adequate protection. Japan is due to receive adequacy recognition during the course of 2018, and South Korea is in the process of seeking adequacy recognition from the European Commission.

13.6. As this is a particularly complex aspect of Data Protection Laws, ***whenever it arises it must be discussed with a member of the Data Privacy Committee.***

14. REPORTING

14.1. In line with CDISC's current Breach Notification Policy (as amended from time to time), all security incidents involving personal data, such as leakage or theft, must be reported **immediately** to a member of the Data Privacy Committee.

14.2. Examples of security incidents which require reporting include :

(i) Theft or loss of computer, external storage medium, multifunctional mobile terminal, mobile phone, or confidential documents containing personal data.

(ii) Publication of personal data without the permission of the Individual.

(iii) Leakage of personal data through Internet via file-swapping software, etc.

(iv) Sending personal data to the wrong recipient in any form including by email, fax and post.

15. AUTHORIZATION

15.1. This document has been approved and is in effect on this date:

Name	Date
Board of Directors	6 May 2019

***

End of Data Protection Policy