ISPE®

Data Privacy: A Compliance Blind Spot

June 2017

A Concept Paper by the ISPE GAMP Community of Practice

Acknowledgements

This Concept Paper was written and reviewed by members of the GAMP® R&D/Clinical Special Interest Group (SIG) of the ISPE GAMP® Community of Practice (COP). It represents industry best practices based on the experiences and input from the individuals listed below and does not reflect the views of any one individual or company.

SIG Chairs

Oliver Herrmann	Q-FINITY Quality Management	Germany
Eric Staib	PRA Health Sciences	USA

SIG Sponsor

Eric Staib	PRA Health Sciences	USA

Document Author

Ian Francis	Novartis Pharmaceuticals AG	Switzerland

Particular thanks go to the following for their support of this Concept Paper:

Frank Henrichmann	PAREXEL International	Germany
Corinne Liabeuf	Johnson and Johnson	France
Arthur (Randy) Perez	Novartis (retired)	USA
Yvonne Rollinger	OmniComm Europe GmbH	Germany
Dieter Wachtmann	PAREXEL International	Germany
Christopher White	Alexion	USA

Table of Contents

Limitation of Liability
In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, or the authors, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

1 Introduction

What should be planned for when implementing a new computerized system, such as a clinical trial database?

For clinical computerized systems, compliance goes beyond Good Clinical Practice (GCP), because these systems frequently process "privacy relevant" data. Controls required by Data Privacy regulations include encryption and restricted access, along with informed consent.

Data Privacy represents legal frameworks that require specific controls for information systems. Challenges with Data Privacy regulation, when compared to Good "x" Practice (GxP) include:

- There is little clear guidance on what is required
- The scope of Data Privacy is often not clear
- Many clinical systems have a multinational or global footprint, requiring data movement across national borders, and the proliferation of privacy laws in different countries can have complex, and sometimes conflicting, implications.

This Concept Paper aims to highlight where Data Privacy regulations could apply, and the requirements for system implementation arising from those regulations.

2 What is private data?

If a computerized system contains personal data, then the system is within scope of Data Privacy frameworks:

> *'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;* [1]

Following from this, it can be deduced that height may be personal data, but it is only privacy relevant if the data subject can be identified, using Personally Identifiable Information (PII). Examples of personally identifiable information include:

- Person's name
- A social security or national identity number
- Employee ID
- A Patient/Subject ID (even if coded/blinded)
- Attributes that, in combination, can uniquely identify a person

The last two examples can cause significant discussion.

It has been assumed that if data is de-identified and uses only a coded (i.e., blinded) Subject ID, the actual person cannot be identified, so the related system will not be privacy relevant. The counter argument (and the legal interpretation) is that there is data **somewhere** that links the Subject ID to an actual person. Even though the data may be found in a different location (such as an investigator site) and it could be difficult to obtain, it is available.

Similarly, single data attributes of a person may not in themselves identify the individual, but sufficient attributes in combination can point to a specific individual, e.g., Date of Birth plus Gender plus Initials plus Zip Code/Postal Code.

However, the use of "Honest Brokers[1]" can remove the burden of Data Privacy regulation from a system that holds only coded patient data by ensuring that a coded ID remains separated from patient identity.

Examples of personal data:

- Last Name
- First Name
- Initials
- Work Address
- Home Address
- IP Address

[1] An "Honest Broker" is an entity that keeps sets of private information but distributes parts of those sets to other entities that should not have access to the entire set.

- Place of Work
- Work telephone, fax, and/or e-mail
- Home telephone, fax, and/or e-mail
- Date of Birth
- Place of Birth
- ID Card Number
- Gender
- Race
- Religion
- Political Affiliation
- Civil Status
- Name of Spouse
- Birth Dates of Children
- Photograph
- Health Data
- Curriculum Vitae

Depending on the country of jurisdiction, these data may be **considered sensitive personal information**, which requires a higher level of control, e.g., race, religion, or political affiliation are considered sensitive in many countries. Health data are also considered as sensitive in many countries, and these data are often collected in the context of clinical trials.

Data for employees, investigators, third party suppliers, and other companies are also covered by Data Privacy, as well as data on patients/trial subjects.

3 The Principles of Data Privacy

The principles described in this ISPE Concept Paper are abstracted from the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [2], with minor modifications to emphasize Computerized System Validation (CSV) considerations.

These principles seem to be, and in many ways are, overlapping or even duplicating and this can cause confusion. This overlap is acknowledged by the OECD [3]. One of the objectives of this ISPE Concept Paper is to condense each principle into tangible and meaningful actions with respect to Clinical Systems implementation.

3.1 Purpose/Specification Principle

> *The purposes for which personal data is collected should be specified at the time of data collection.* [2]

This principle requires that a data controller states what they plan to do with the data, at the latest when it is collected.

In clinical trial data management systems, the purpose of collecting private data should be defined in the protocol and outlined in the informed consent. Companies should consider those purposes when designing databases that process data.

For other types of system (those without an informed consent), a documented Privacy Statement may be needed to explain the purpose, and could lead to functional impacts on a system, such as a statement of purpose on a system log in screen.

3.2 Use Limitation Principle

> *Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle, except with the consent of the data subject or by the authority of law.* [2]

This principle requires that a data controller does not use the data for purposes other than those specified.

Although this may initially seem to duplicate the Purpose Specification Principle, there is a subtle difference. Data can be used in many specific ways to support a general purpose. For example, a patient's personal details (e.g., home address, blood pressure) collected as part of a clinical trial can be used in the analysis of the clinical trial, but may also be used to support a recall if a problem is found with the products used in the clinical trial. Typically, both of these *uses* would be permitted by the *purpose* of running a trial; however, secondary use of data that is **not** specified by the *purpose* requires either additional consent, or investment in anonymization processes and tools to make the data non-privacy relevant.

When a system is planned to contain PII, the use of the data (User Requirements) should be compared with any purpose/consent statement related to the data, or consent should be obtained from the data subject.

Any request for a new use of the data needs to have a careful assessment with respect to the purpose specification and consent granted.

3.3 Collection Limitation Principle

> *Data controllers must limit their collection of personal data to the minimum needed to meet the purpose consented to and the applicable local laws.* [2]

Consent may be implicit or explicitly obtained; however, persons who provide personal data should do so willingly and consciously. This consent provides the legal basis for allowing the data to be collected and sets the legal boundaries on what may be done subsequently with that data.

System documentation should define what data will be collected. The System Owner should be able to justify any PII that is collected in relation to the consent.

3.4 Data Quality and Integrity Principle

> *Personal data should be relevant to the purposes for which it is to be used and needs to be accurate, complete, and current.* [2]

This principle has two aspects:

1. **Quality:** having correct data, e.g., a person's name, age, and gender are all correct

2. **Integrity:** ensuring that the data quality is maintained throughout the life time of the data

This is where there is the most obvious overlap between the objectives of CSV and Data Privacy. It is widely accepted that validation is the process by which to provide evidence that a system ensures data quality and integrity. Systems maintaining personal data should be validated accordingly, depending on the type and extent of data being processed. The GAMP® risk-based approach can be applied to scale validation activities to fit the needs of specific computerized systems.

3.5 Security Safeguards Principle

> *Personal data should be protected by reasonable security safeguards against risks such as loss or unauthorized access to data, as well as destruction, use, modification, or disclosure of personal information.* [2]

This principle encompasses all elements of information security and information life cycle management, including:

- Access control (physical and logical, segregation of duties)
- Audit history
- Disaster recovery
- Backup/restore
- Secure data decommissioning process
- Security Breach Plan to handle disclosures

Security controls should be commensurate with risk. For example, sensitive PII may require encryption both at rest and in transit. Non-sensitive PII may require only appropriate access controls.

3.6 Openness Principle

> *There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.* [2]

This principle imposes a responsibility on the data controller to provide a (documented) mechanism for data subjects to request and receive information about the data held about them.

The data subject should have a way to request information from the data controller about their own data and its use. The data controller, in this context, is usually the regulated company (legal entity) rather than an individual, because within the regulated company there will several individuals responsible for the data.

This requires that the regulated company know what data they control and know where it is located. It can be easy to lose track of data and its locations in larger regulated companies with large amounts of data and multiple databases. An inventory of private data types, databases, and responsible data owners is the considered a simple means to have the ability to respond to requests from data subjects in a timely and accurate manner (also see Section 4 on Local Regulations).

3.7 Individual Participation Principle

> *An individual has the right:*
>
> *a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;*
>
> *b) to have communicated to them, data relating to them within a reasonable time;*
> - *at a charge, if any, that is not excessive;*
> - *in a reasonable manner; and*
> - *in a form that is readily intelligible to them;*
>
> *c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and*
>
> *d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.* [2]

This principle outlines the rights of the data subject, and as such is an extension of the Openness Principle, with similar implications on the data controller.

3.8 Accountability Principle

> *A data controller should be accountable for complying with measures which give effect to the principles stated above.* [2]

The data controller should decide about data and data processing activities. Processing of data is performed for the benefit of the data controller. Accordingly, accountability for complying with privacy protection rules and decisions should be placed on the data controller. Accountability should remain with the data controller even if the processing of data is performed by another party, such as a Contract Research Organization (CRO).

The regulated company should have both its own data privacy framework established and should also perform due diligence on third parties which process private data. For example, supplier assessments should be performed to ensure that a third party has adequate data privacy controls established.

4 Local Regulations

The principles described in this ISPE Concept Paper lead to specific controls, or requirements, for deploying and using clinical systems, and generally apply across all Data Privacy regulations. Specific local regulations may also need to be considered. Regulated companies may employ an expert in this area to identify the regulations and related controls.

For example, Switzerland requires a regulated company to either:

a. “declare” their intention to “open a data file” (i.e., create a system to contain privacy-relevant data) *before they are opened*

OR

b. to employ a designated data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files [4]

For a large regulated company with many clinical systems, the former option is unlikely to be efficient. Where the second option is employed, this results in an inventory of privacy relevant systems. Having an inventory of privacy relevant systems is a requirement common to many jurisdictions.

5 Cross Border Transfers

Transferring data across national borders has several legal implications, dictated by national privacy regulations. This imposes legal/contractual obligations on the data controller but does not add any additional requirements for systems implementation or validation.

In general, transferring data across national borders (or outside regional jurisdictions such as the European Economic Area (EEA)) is not permitted unless specific conditions are met.

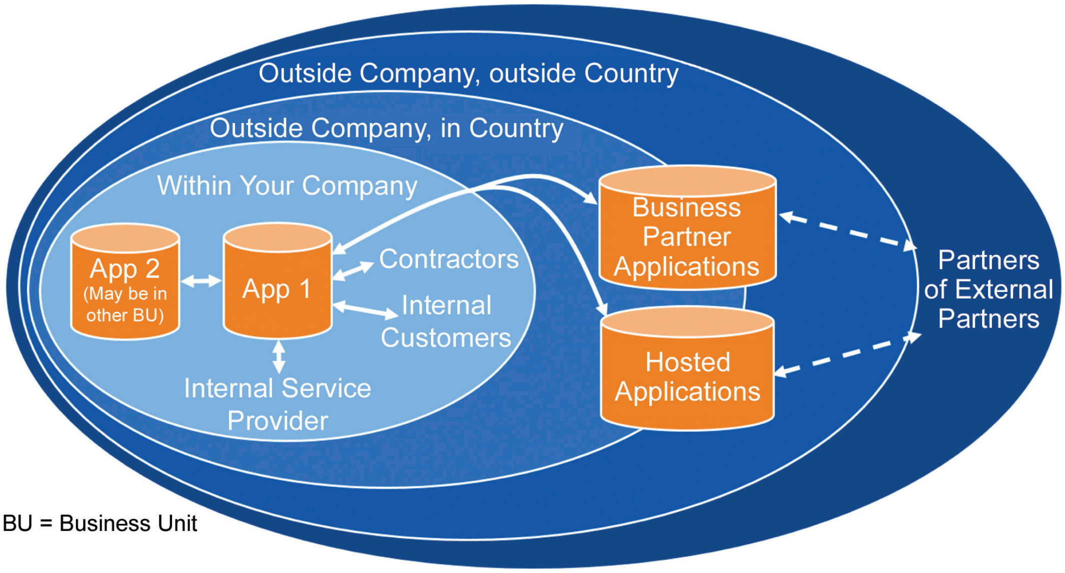
Note: in this context "transfer" does not necessarily mean the physical movement of data from one location to another. Data viewed on screen is considered "transferred".

Data may be transferred to:

- Countries that are considered "Adequate" for the transfer of personal information. Adequacy is determined by the regulatory authority:
    - For example, for European Union (EU) Member states the following are considered adequate:
        - Switzerland, Canada (with regard to transfers made to recipients subject to the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) [5], Argentina, the Bailiwick of Guernsey, the Isle of Man, and the Bailiwick of Jersey.
- Data may be transferred if the following have been executed:
    - Standard contractual clauses, e.g., in the EU so called Model Clauses approved by the EU Commission
    - Ad hoc data transfer agreements
- Data may be transferred if an exception has been met, e.g.:
    - Consent of the Data Subject – only for limited transfers
    - Transfer is necessary to fulfill a contract with the Data Subject
    - Transfer is required by law

Understanding how data flows is considered critical to understanding how Data Privacy will apply.

Figure 5.1: ***You can't manage privacy without managing the data*** **[6]**


Outside Company, outside Country
Outside Company, in Country
Within Your Company
App 2
(May be in other BU)
App 1
Contractors
Internal Customers
Internal Service Provider
Business Partner Applications
Hosted Applications
Partners of External Partners

BU = Business Unit

5.1 Cloud Solutions and Borders

The location of data processed in the cloud may not be well defined for cloud computing solutions. Cloud based services should be carefully examined to determine their legality regarding processing private data [7].

Aspects that should be understood when managing personal data in the cloud include:

- Where is the physical equipment on which the data is stored?
- Where are the users accessing the data?
- Where are the people supporting the database and what can they see?

Established cloud service providers may recognize these challenges and provide solutions to facilitate compliance [8].

6 Penalties

An amendment to the European General Data Protection Regulation [9] is currently progressing through the European Parliament that, if it is enacted, would mean that regulated companies could be fined **5% of their global turnover** in the event of a serious data breach.

For a global Pharma company 5% of turnover could be in the order of **$1 (US) Billion!** [10]

Note: This paper does not intend to explain all the requirements of the Data Privacy law, and does not represent legal advice.

Legal advice from a qualified Data Privacy Officer should be obtained before making decisions on the use of private data and data privacy relevant computerized systems.

7 Case Studies

The following case studies provide real world examples of how data privacy principles and regulation affect clinical systems.

Scenario	Privacy Considerations	Key Principles to be Considered	Requirements
Extending Data Access to our Statisticians in India (simple scenario) We are implementing a clinical trial database. It will be hosted in Switzerland, and have users locally. It will be accessed via an internal web-based application. Our statisticians in India will need access to start analyzing the study data.	Even though the users in India work for the same "Company" they are based outside of the EEA and, therefore, providing them access to the data constitutes a cross border transfer of data. Even though the data does not actually move and all analyses and resulting data remain in Switzerland, the data is displayed on screen in India, and this is considered data transfer. In this example, cross border transfer agreements would be required before access is granted. This requires system access procedures to ensure data privacy requirements are met. Also, training and privacy awareness of the permitted use of the data must be provided to all users.	• Use Limitation • Security Safeguards • Local Regulations • Cross Border Transfers	• Registration of the database in an inventory • Data Transfer Agreements • Access control procedures • Privacy Policy/ Training
Extending data access to our Statisticians in India (Complex, *real* scenario) Mega Pharma Co. is conducting a global clinical trial. EU trial data will be stored in trial systems in Switzerland and US data centers. Mega Pharma Inc. (the US affiliate of Mega Pharma Co.) processes data as part of this trial in the US databases. Mega Pharma Inc. decides to transfer some of the processing of trial data to Mega Pharma Ltd. India. Mega Pharma Ltd. India hires a sub-contractor to manage some of the data entry into the systems.	• Transfer of EU trial data to Mega Pharma Co. is permitted since Switzerland is considered adequate for the transfer of personal data and the patients have signed an informed consent. • Transfers from Mega Pharma Co. to Mega Pharma Inc. are permitted since Mega Pharma Inc. is US-Swiss Safe Harbor certified and patients are aware of transfers through informed consent. • In order to transfer data to India, Mega Pharma Inc. must otify Mega Pharma Co. of the transfer and Mega Pharma Co. must agree to that transfer prior to providing access to Mega Pharma Ltd. India. Mega Pharma Co. must notify the other Pharma sites that their data is now moving to India. • Mega Pharma Inc. must enter and execute a processing agreement with Mega Pharma Ltd. India providing for an adequate level of protection similar to that required by Mega Pharma Inc. under the Safe Harbor. • Mega Pharma Inc. must either execute an agreement with the Indian third party or must ensure that the third party has an appropriate agreement with Mega Pharma Ltd. India.	• Use Limitation • Security Safeguards • Local Regulations • Cross Border Transfers	• Registration of the database in an inventory • Data Transfer Agreements • Access control procedures • Privacy Policy/ Training • Supplier Audits to ensure equivalent security/privacy requirements are established at the third party

Scenario	Privacy Considerations	Key Principles to be Considered	Requirements
Consolidating and Aggregating Data A data warehouse is planned that will consolidate data from multiple clinical trial databases. The purpose is to support a product recall across all studies.	For this purpose, only limited data is required, e.g., gender is probably not required in the data warehouse, because it is not relevant to conducting a product recall. The data will require some coded health information (Subject ID, Treatment Arm) to enable a recall to be made.	• Collection Limitation • Data Quality and Integrity	• Data Specification • Validation of system • Data encryption in transit and at rest
Identify subjects for a new trial from existing trials A clinical trial database contains patient data, including Patient ID, gender, location (Zip Code/Post Code) and health data. It is used for statistical analysis for efficacy, etc. The Clinical Trial Planning group wants to find subjects for a new trial. They would like to use the existing clinical trial database to identify candidates for the future trial.	This would normally be outside the purpose of the informed consent for a trial; the purpose of collecting the data is to run a clinical trial, not to identify candidates for future trials. To be able to use the subjects' data in this way, the subjects must be contacted to obtain additional consent that their data can be used for the new purpose.	• Purpose Specification • Use Limitation • Openness	• Additional explicit consent from subjects for this new use of the data.
Mergers, Acquisitions and Divestments The Mega Pharma Oncology Development division is sold to another company, Acme Pharma. The clinical trial data for this division is stored in the corporate clinical trial database, along with trial data from other divisions.	The data related to the Oncology trials now belongs to Acme Pharma. The subjects must be aware that the data controller has changed and any change in the process to access their information.	• Data Quality and Integrity • Openness	• Data will require validated extraction and transfer to the new data controller, and secure disposal from the original controller, who is no longer permitted to hold the private data. • Data subjects must be notified of the change of data controller and processes related to data access.

Scenario	Privacy Considerations	Key Principles to be Considered	Requirements
Copying Production Data into a Test or Training System The clinical data management system has been established and validated. A Protocol change requires a change in an electronic Case Report Form (eCRF). The system support team wants to copy the current production database into the Quality Assurance (QA)/test system to verify that new eCRF functions correctly. When the change to eCRF has been validated, the support team want to copy the eCRF and all the data into a training database for training the end users with "realistic" data.	This would not normally be a permitted use of the data for operating a clinical trial. Test or training systems often have less rigorous access controls implemented, meaning that disclosure of private data to unauthorized individuals will be highly likely. Similarly, data protection mechanisms, such as strong password controls, encryption, or segregation of duties may not be applied, leading to risks of security breaches and unblinding or other data exposure. To allow for this scenario, the systems would all need to be managed to the same standard and with the same controls established as the productive system. Additionally, additional consent may be required from the subjects. This is often cost prohibitive with the result that either data is de-identified or dummy data sets are used.	• Purpose • Use Limitation • Security Safeguards • Openness	• Data Specification • Validated process for data identification
Outsourced Data Collection A CRO collects trial data, consolidates and transfers to the sponsor company.	Even though the CRO collects and manages the data, the company is still accountable that all privacy principles are established.	• Accountability • Security Safeguards	• Privacy assessment to determine and establish adequate data privacy controls at third-party • Secure (encrypted/ signed) connections/ data transfer between third party and data controller.

8 References

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046.

2. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development (OECD), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

3. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Explanatory Memorandum, Organisation for Economic Co-operation and Development (OECD), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum.

4. Swiss Federal Act on Data Protection (FADP), Art. 11a Register of data files, https://www.admin.ch/opc/en/classified-compilation/19920153/index.html#a11a.

5. Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), http://laws-lois.justice.gc.ca/eng/acts/P-8.6/.

6. Graphic representation originated by Dr. Arthur Perez.

7. Guide to Cloud Computing, Swiss Federal Data Protection and Information Commissioner (FDPIC), https://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=en.

8. Regions and Availability Zones, example Amazon Web Services, https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html.

9. European General Data Protection Regulation (GDPR), http://www.eugdpr.org/.

10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679.

9 Glossary

9.1 Acronyms and Abbreviations

CRO	Contract Research Organization
CSV	Computerized System Validation
DPA	Data Protection Authorities
eCRF	electronic Case Report Form
EEA	European Economic Area
EFTA	European Union Free Trade Association
EU	European Union
FAQ	Frequently Asked Questions
FDPIC	Federal Data Protection and Information Commissioner (Switzerland)
GCP	Good Clinical Practice
GDPR	General Data Protection Regulation (Europe)
GxP	Good “x” Practice
HR	Human Resource
IT	Information Technology
OECD	Organisation for Economic Co-operation and Development
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
QA	Quality Assurance
US	United States

9.2 Definitions

Access

The right of the Data Subject to request and obtain from the data controller information regarding his/her personal data which is subject to processing, at least as to the purpose of the processing, the categories of personal data concerned, as well as the origin of such data and its disclosure or intended disclosure. The Data Subject is also entitled to any other access right conferred to them under local applicable laws. For example, an employee could request access to his personal file; a customer of a company could request access to all the personal data that the company holds about them.

The Data Subject can request the rectification, erasure and blocking of personal data, if the processing of such data does not comply with privacy guidelines or is incomplete or inaccurate.

Anonymization/Anonymized Data

Any data which are irreversibly stripped of any identifiers and can no longer be linked to an individual and is therefore not considered being personal data.

Coded Data

Data collected for research purposes that are indirectly identifiable by replacing the personal identifiers with a code or random number. Coded data may be re-identified and linked to a specific research participant via a trusted third party such as an independent researcher. In many instances and according to local laws and regulations, coded data may be considered personal information under local laws and regulations.

Consent

Any specific and informed indication freely given by the individual concerned signifying his/her clear and unambiguous agreement to have his/her personal data processed. Depending on the type of information and local requirements, consent must be explicit and specific (Opt-in) or implicit (Opt-out).

Database

A structured set of data which is arranged in a systematic or methodical way, and is accessible by electronic or other means according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis

Data Controller

The person, public authority, agency, or any other body which alone or jointly with others determines the purposes for which and manner in which, any personal data is, or will be processed; where the purposes and means of processing are determined by national or community laws or regulations, the Controller or the specific criteria for his nomination may be designated by national or community law. Most data protection obligations must be met by the Controller and in most cases, Controllers are liable for data protection violations.

Data Protection Authorities (DPA)

Authorities in each EU member state, as well as in other countries (if applicable). responsible for ensuring compliance with data protection legislation. The authorities have powers to investigate whether companies (or public administration) are in compliance with the law and to impose heavy fines for non-compliance.

Data Protection Legislation

A set of rules that regulate the protection of personal data. Usually this legislation is contained in various legal instruments, including secondary legislation.

Data Subject

The identified or identifiable person whose personal data are processed; an identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (including a social security number or a code in a clinical trial case report form in combination with other information).

Disclosure

The accessibility of personal data to any person or entity other than the Data Subject, Controller, or Processor. This may include, but is not limited to, the active transfer of personal data to company affiliates or third parties distributing or publishing the personal data, through manual, electronic or verbal means and viewing or access the data which is made available for view or access.

European Economic Area (EEA)

The Agreement between the European Union and the European Union Free Trade Association (EFTA) entered into force on 1 January 1994 and includes the EU member states, Norway, Iceland, and Liechtenstein.

European Union (EU)

The European Union, including as of May 2004 the following countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

Individual

The Data Subject.

Information

The information provided to the Data Subject whose personal data are processed in regards to:

- The identity of the Controller and of his representative, if any
- The purposes of the Processing for which the personal data is collected
- Any further information concerning the specific circumstances under which the data are collected such as:
  - The categories of data concerned
  - The recipients or categories of recipients
  - The existence of the right of access to and the right to rectify the data concerning him/her

Information System

An organized assembly of computing and communication resources and procedures (i.e., equipment and services, together with their supporting infrastructure, facilities, and personnel) that create, collect, record, process, store, transport, retrieve, display, disseminate, control, or dispose of information to accomplish a specified set of functions.

Infrastructure

Electronic information and communications systems and services, and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information.

Legitimate Business Purpose

A purpose which is directly or indirectly related to the business operations of the Controller, and which does not interfere with the fundamental rights and freedoms of the individual. For example, Human Resource (HR) managers may process personal data to perform their administrative obligation. A legitimate business purpose may include compliance with legal, regulatory, or ethical obligations applicable to the regulated company.

Model Clauses

The European Commission’s pre-approved contractual agreements that may be used as is (no material additions can be added) to legalize a data Transfer.

Opt-in Consent

A system whereby Controllers obtain clear and specific consent from the individual before the individual’s personal data is, collected, processed, or otherwise used, for a particular purpose. The opt-in consent is given by an affirmative act and must be in writing or by other verifiable means, such as clicking a box on an online form.

Opt-out Consent

A system whereby Controllers deem consent to have been given unless an individual specifically refuses to have his/her personal data processed, or otherwise used, for a particular purpose. Opt-out consent is given by failing to take action, such as not un-clicking a box on such a form.

Personal Data/Personal Information

Any information relating to a Data Subject. Personal information includes, without limitation, electronic data and paper based files that include information, such as name, home address, office address, e-mail address, age, gender, family information, profession, education, professional affiliations, and salary. Sensitive personal information (sometimes also called Special Categories of Personal Data) are a subset of personal information as defined below. Local laws may classify further data types as personal information.

Process/Processing

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Processor

The natural or legal person, public authority, agency or any other body, which processes personal data on behalf and under instructions of the Controller. The Processor is, typically, not subject to the same obligations as the Controller

Recipient

A natural or legal person, public authority, agency or any other body to whom personal data are disclosed, including but not limited to third parties.

Safe Harbor

A self-certification process established by the EU Commission and the United States Department of Commerce. It is one of several data transfer methods by which companies located in the United States can legally receive personal data from the EU. US companies have the option to self-certify to the EU-US Safe Harbor Framework and/or Swiss-US Safe Harbor Framework. Certification allows US companies to access personal information from the EU and Switzerland. The Safe Harbor Principles and Frequently Asked Questions (FAQ) as well as a list of Safe Harbor certified companies can be found at www.export.gov/safeharbor/.

Sensitive Personal Information/Data

Personal data (sometimes also called Special Categories of Personal Data) that reveals a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, social security, criminal charges and conviction/sentence, or a person's sex life or health, including data collected in clinical trials.

In certain jurisdictions, such as Switzerland the collection of personal data which allows the appraisal of the essential characteristics, traits and personality of an individual, is protected like Sensitive Personal Data. For employee personal data, this includes the individual's qualifications, performance, and behavior at work as well as assessment by handwriting experts. In jurisdictions, such as the United States, this would include credit card information, social security numbers, and other government identifiers such as passport or visa numbers.

System Documentation

The files and documents created and stored during the creation and development of an Information System to certify and maintain evidence of the existence and compliance of the Information System itself.

Transfer

The disclosure of personal data carried out by any person other than the Data Subject. This includes a transfer within the Controller's entities and departments, and third parties outside.

ISPE®

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

www.ISPE.org