Impelsys

GDPR (REGULATION) & PIMS (BS 100012 STANDARD) OVERVIEW

Spreading Knowledge Through Technology

Impelsys

Topics

- Introduction to GDPR
- GDPR Compliance
- GDPR Principles
- GDPR Articles
- PIMS
- Explore PIMS & GDPR
- Contact

Introduction to GDPR

Impelsys

GDPR OVERVIEW

- General Data Protection Regulation (GDPR)
- What:
  - It is regulation in European Union (EU) law.
  - It is a Data Privacy
  - Protects the EU natural person personal data
  - Replaces: Data Protection Directive
  - Implementation date: 25 May 2018
- Whom will apply:
  - All, who collects and process the EU residents data, within or outside EU region.
- What we should do:
  - Adopt and compliant to GDPR principles
  - Adhere and compliant to GDPR Articles (only for applicable out of 99)
  - Be aware of Administrative fine, penalty
- Consequences of Non compliance to GDPR
  - Reputational loss
  - Lose existing & new customers
  - Fine for violations – can go up to 20 million or 4% global annual turnover of preceding year (which ever is higher)

Privacy is the right to be let alone or freedom from interference or intrusion.

What is Privacy

Three elements in privacy

- Secrecy
- Anonymity and
- Solitude

Privacy could be

- Information privacy (collection and handling of personal data
- Territorial privacy (intrusion into the environment – home, workplace etc.,)
- Bodily Privacy (body cavity searches, genetic testing, drug testing etc.,)
- Communication Privacy (protecting means of – email, telephone, postal etc.,)

Privacy is the right to be let alone or freedom from interference or intrusion.

Impelsys

Background of GDPR

1995 - The Data Protection Directive is a European Union directive which regulates the processing of personal data within the European Union.

It is an important component of EU privacy and human rights law.

2012 - The EU has realized that while technology has evolved drastically in the last few decades, privacy laws have not. European Commission set out plans for reforming data protection across the European Union in order to make Europe 'fit for the digital age'.

2016 - Reformed as General Data Protection Regulation (GDPR)

May 25, 2018 - GDPR enforceable.

What's in GDPR

Impelsys

- Protection of natural persons with regard to the processing of European Union (EU) personal data and rules relating to the free movement of EU personal data.
- It protects fundamental rights and freedoms of EU residents.
- Who does apply to: GDPR applies to any organization that works with the personal data of EU residents.
- Where does apply: This law doesn't have territorial boundaries. It doesn't matter where your organization is from — if you process the personal data of subjects of the EU, you come under the jurisdiction of the law.
- What is personal data: Any information relating to an identified or identifiable natural person. The identifiers are classified into two types: direct (e.g., name, email, phone number, etc.) and indirect (e.g., date of birth, gender, etc.).
- Who are key players:
  - Data subject - A natural person residing in the EU who is the subject of the data.
  - Data controller - Determines the purpose and means of processing the data.
  - Data processor - Processes data on behalf of controller.
  - Supervisory authorities - Public authorities who monitor the application of the regulation.

What's in GDPR

Impelsys

- What should do:

  Adopt and compliant to GDPR principles

  Adhere and compliant to GDPR Articles (only for applicable out of 99)

  Be aware of Administrative fine, penalty

- Any penalty for non-compliance: A breach of the GDPR incurs a fine of up to 4% of annual global turnover or €20 million (whichever is greater).

- What is breach: Violation of GDPR, principles or articles
  - Eg : excessive data collection, prolonged retention of data, lost of data. Controllers must notify the stakeholders (the supervisory authority, and where applicable, the data subjects) within 72 hours of becoming aware of a breach.

- What is New in GDPR from previous directive:
  - *More power (control) to the data subjects* : Right to be informed, Right of access, Right of rectification, Right to erasure, Right restrict, right to data portability etc.,
  - stressed more on *privacy by design*
  - Makes more *data security*
  - Keep *record of everything* ie from collection t processing to finally disposing
  - Address the *cross border data transfers*

GDPR is constituted with 99 Articles & 173 Recitals.

These Articles regulates the rules of GDPR to be followed and compliant.

GDPR **principles**, **Rights of Data subject**, **Role & Responsibilities** of controller, processor, data protection officer, Supervisory authority. Transferring of personal data, **Security in Processing**, Data Protection impact **assessment**, codes of conduct, **breach notification and penalties**.

PERSONAL DATA OR PERSONALLY IDENTIFIABLE DATA (PII)

Impelsys

Full Name
Email address
Home address
Status
Date of Birth
National ID Numbers
Social Security Numbers
Passport Number
Events Attended
Location Information
Driver's License number
Visa Permit Number
What are you doing when/status
Sexual orientation
Gender
Vehicle registration plate number
Disability information

Criminal Record
Photos
Salary
Grades
Education History
Place of Birth
Employment History
Job Position
Mother maiden name
Generic information
Insurance details
Medical information
Credit card Number
Places visited
Air ticket bookings

Work details (company name, address, phone number)
Family members details
Dependents
Email Address
Password
Digital Identity
Bio Metric data – retina, face, fingerprints, handwriting
Cookies
Password hashes
Session information
Friends Name
Social Networking sites usage
Membership details

Key requirements of GDPR

Impelsys

- Data Protection Officer
- Data Transparency
- Consent
- Data Protection Impact Assessment
- Data Subject Rights

- **Data Protection Officers (DPO):** DPOs must be appointed where the core activities of the organization involve “regular and systematic monitoring of data subjects on a large scale” or where the entity conducts large-scale processing of “special categories of personal data.”
- **Data Transparency:** GDPR requires certain information be made available at point of data collection. This may include the identity and contact information of the organization/DPO, the purpose and legal basis of the data processing, and the rights afforded to the data subject.
- **Consent:** A data subject’s consent must be freely given, specific and informative, and expressed by either a statement or affirmative action.
- **Data Protection Impact Assessment (“DPIA”):** Any organization whose activities are likely to result in a high risk to the rights and freedoms of individuals must conduct a DPIA before proceeding with the activity.
- **Data Subject Rights:** GDPR gives data subjects the rights to erasure, rectification, portability, and objection to processing.

Key requirements of GDPR

Impelsys

- Data Security
- Subject Access Requests
- Data Portability
- Privacy by Design
- Data Export to third countries
- Breach Reporting

- **Data Security:** Personal information must be pseudonymized and encrypted.
- **Subject Access Requests/Data Portability:** Individuals are permitted to request details regarding the information collected from them and how the data is being used. Data must be provided in a structured, commonly used, and readable format.
- **Privacy by Design:** Organizations are required to design privacy policies, procedures, and systems at the early stages of any product or process development.
- **Data Export to Third Countries:** Data can be transferred outside of the European Union under a Commission adequacy decision, standard contractual clauses, and binding corporate rules (BCR)
- **Breach Reporting:** In most cases, data breaches must be reported to the relevant data subjects and regulators without undue delay (within 72 hours, where possible).

Impelsys

Basic Terms & Definitions

- Personal data or Personally identifiable information (PII) - any information relating to an identified or identifiable natural person ('data subject');

  Example:

  direct identifiers – Account information, email, phone number etc.,

  Indirect identifiers – age, data of birth, gender etc.,

- Special Categories of personal information – Racial or ethnic origin, political opinions, religious beliefs, trade union membership, processing of genetic information, information concerning health or self life.

- Processing - any operation or set of operations which is performed on personal data or on sets of personal data - such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- Profiling – Form of automated processing of personal information consisting of the use of personal information to evaluate certain personal aspects relating to data subject . Eg: personal preference, interests, behavior etc.,

- Consent of the data subject - any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

- Pseudonymization – processing in a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information provided additional information are kept secret.

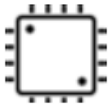
- **Third party** - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
- **Controller** - the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- **Processor** - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **Recipient** - a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- **Personal data breach** - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **Supervisory authority** - an independent public authority which is established by a Member State.
- **Vital interests -** Processing is necessary to protect life and death of an individual.
- **Legitimate interests -** Processing is necessary under union or state law and disclosing.

Key Players in GDPR

Impelsys

Data Subject - an individual who is the subject of personal data

Data Controller - a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data



Data Processor - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Sub Processor / Third party - a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data

Joint Controllers - two or more controllers who jointly determine the purposes and means of processing

Supervisory Authority - independent public authority which is established by a Member State to monitor consistent application of the laws

Representative - a natural or legal person established in the European Union who, designated by the controller or processor represents the controller or processor with regard to their respective obligations

GDPR Compliance

Impelsys

How to be compliant with GDPR

Impelsys

- Respecting the European Union GDPR regulation
- Knowing the Consequences of Non compliance to GDPR
- Respecting the privacy, rights and freedom of European Union residents personal information
- Understanding the requirement or scope of ‘data protection’
- To enhance our trust, relationship and value our beloved customer & clients to expand the business and services

We need to be compliant with GDPR.

- What should do to have compliant with GDPR:
  - Adopt and compliant to GDPR Principles
  - Adhere and compliant to GDPR Articles (only for applicable out of 99)
  - Adopt & Establish the Personal Information Management System (PIMS) and supportable standards.

GDPR Principles

Impelsys

GDPR 6 Principles

Impelsys

Impelsys

PRINCIPLE – 1

LAWFULNESS, FAIRNESS AND TRANSPARENCY

- Processing shall be lawful only if and to the extent that at least one of the following applies:

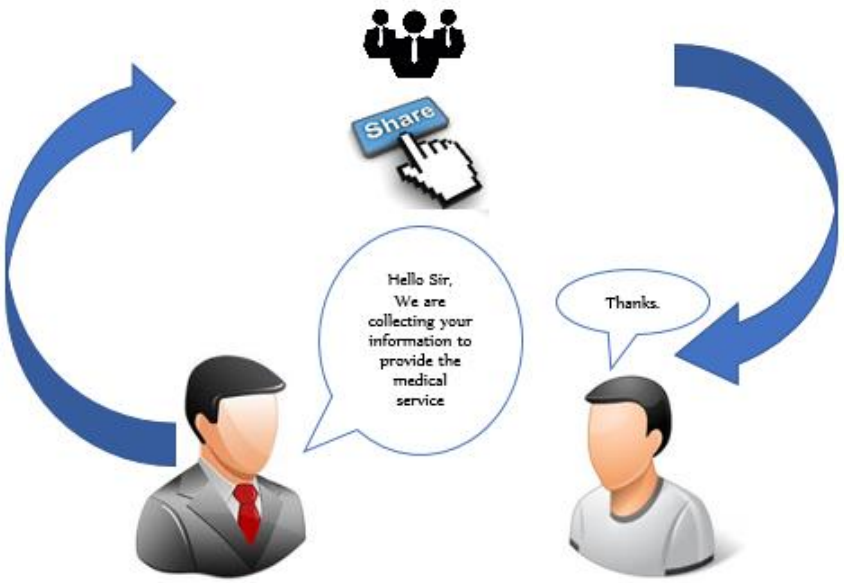
  - ✓ Data subject has given consent to the processing - one or more specific purposes;
  - ✓ Processing is necessary for the performance of a contract;
  - ✓ Processing is necessary for compliance with a legal obligation to which the controller is subject;
  - ✓ Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  - ✓ Processing is necessary for the performance of a task carried out in the public interest;
  - ✓ Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

Example:

1. Obtain fairly by the tax authorities from an employer for legal (no consent from DS).
2. Disclosing of patient's medical records after diagnosis under vital interest of DS.

Personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject.



PRINCIPLE – 2
PURPOSE LIMITATION

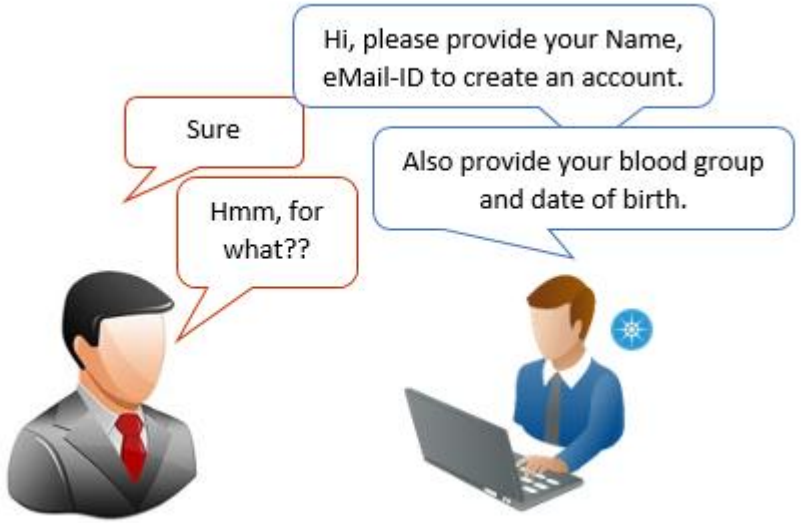
Personal data shall be:

Collected for specified, explicit and legitimate purposes only.

- Personal data collected for specified purpose should not be further processes that is incompatible with those collected purpose.
- Further processing means it can be for statistical purpose or historical research purposes.

Example:

1. General Practitioner discloses the data subjects personal records to some travel agency to enhance holiday packages. This violates the purpose limitation.



- Collect the relevant personal information which is necessarily required for purpose of processing.
- Don’t collect unnecessary information.

PRINCIPLE – 3
DATA MINIMIZATION

Personal data shall be:

Collect only adequate, relevant and limited information what is necessary for the purpose of processing.

PRINCIPLE – 4

ACCURACY

Personal data shall be:

Accurate, kept up to date, rectify inaccuracy and rectified without delay.

- Personal data should be accurate, kept up to date.
- Ensure that inaccurate data is rectified and corrected immediately.

PRINCIPLE – 5

STORAGE LIMITATION

Personal data shall be:

Kept in a form which permits identification of data subjects for no longer than for the purpose for which personal data is processed;

- Ensure only for the specific period for what purpose of processing should be stored.
- Personal data stored accordance with any **legal or law obligations**.
- Beyond the purpose of processing, data should not be stored for further other means of processing.

Example:

1. Tax information of employees data of a Employer should be retained for minimum 7 years as per Tax Authority Law.

Impelsys

PRINCIPLE – 6

INTEGRITY AND CONFIDENTIALITY

01 **CONFIDENTIALITY**

Confidentiality prevent unauthorized disclosure of information.

02 **INTEGRITY**

Integrity assure that data cannot be modified in an unauthorized manner.

03 **AVAILABILITY**

Information should be readily available for authorized users.

- Ensure personal data is protected against unauthorized or unlawful processing.
- Ensure there is no accidental loss of data, destruction or damage of data.
- Ensure technical measures are taken to protect the personal data.

Personal data shall be:

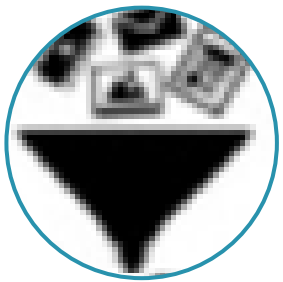
In a manner that ensures appropriate security techniques are applied and measures are taken care.

Accountability

The Controller is responsible for and be able to demonstrate the compliance with GDPR.

Lawful, legal and transparent processing

Purpose Limitation



Data Minimization

Data Accuracy

Storage Limitation

Confidentiality and Integrity

GDPR Articles

Impelsys

GDPR Articles

Impelsys

- GDPR consists of Articles and Recitals. 99 Articles and 173 Recitals.
- **Articles** are written statements, containing a series of rules and stipulations of GDPR law.
- **Recital** a recital is a text that sets out reasons for the provisions of GDPR law.
- Explore and Be aware of these articles and Recitals.
- Adhere to Articles. Not all, but all necessary for the organization to be compliant.

- Refer the websites - https://gdpr-info.eu/ , https://ico.org.uk

PIMS

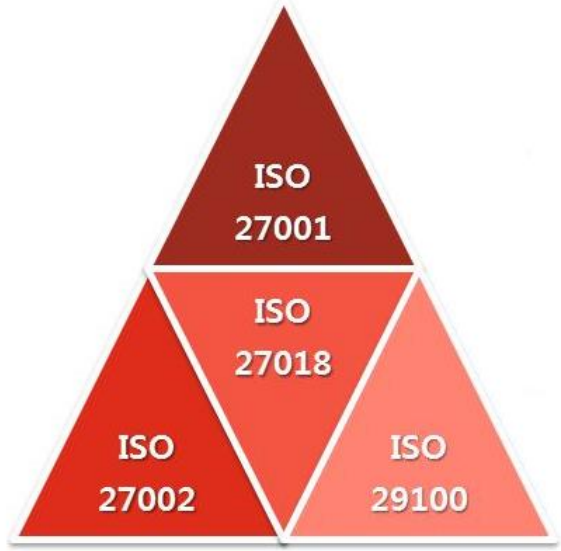
Impelsys

Personal Information Management System (PIMS)

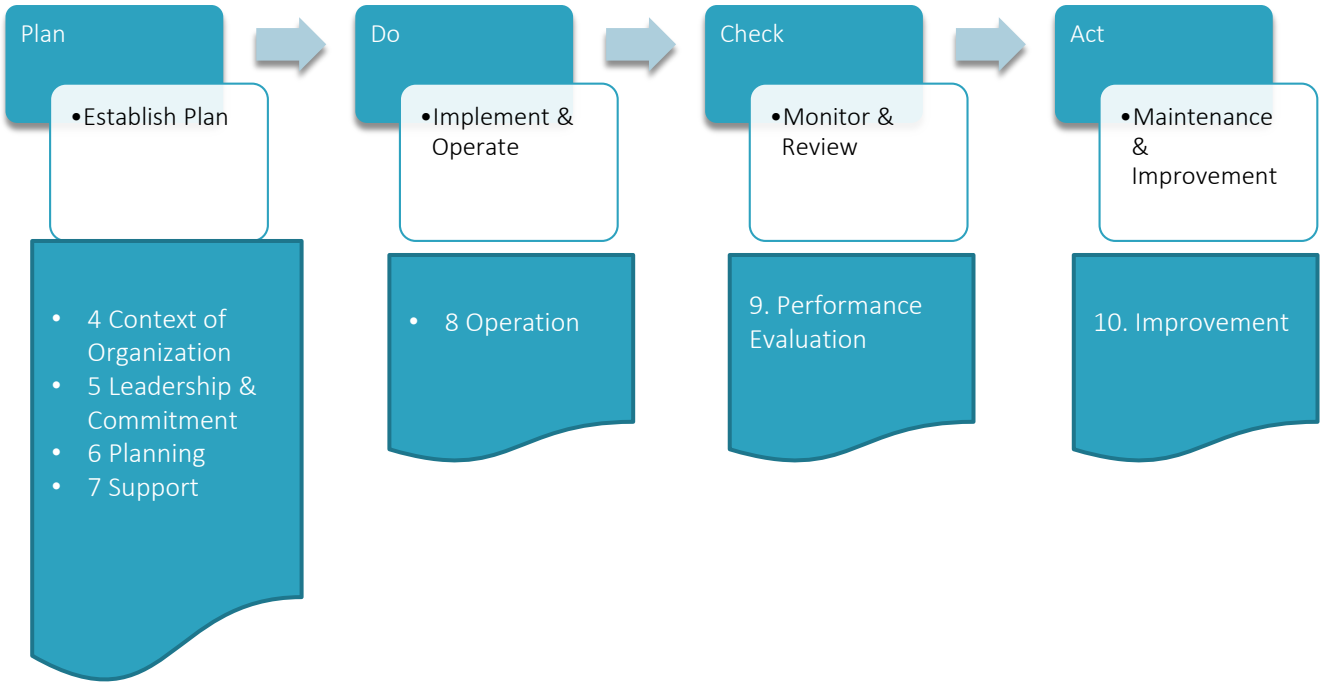
Impelsys

- Establish and Implement PIMS as per BS 10012 & GDPR Standard.
  - Policy, Process, Procedures, Guidelines and checklists

- Supportive Standards to be referenced are:
  - ISO 27000 series :
    - ISMS 27001 - Information Security Management System
    - ISO/IEC 27018:2014 - Protecting PII in public cloud service (AWS)
  - ISO 29100 series :
    - 29001 - Data privacy and Security Techniques, 29151 - Data Security and Data Privacy - Cor
    - 29134- Data Privacy Impact Assessment



PIMS Structure



PIMS Manual

0	Introduction
1	General
2	Data Protection Principles
3	Notification
4	Context of Organization
5	Leadership
6	Planning
7	Support
8	Operation
9	Performance Evalution
10	Improvement

Explore PIMS and GDPR

Impelsys

Legal Basis and lawful processing

Impelsys

- Consent
- Contract
- Legal Obligation
- Vital Interest
- Public Interest
- Legitimate Interest

Refer Legal basis processing procedure and checklist
Refer contracts / agreements

- Ensure data processing on the ground of legal and lawful basis.
- Consent obtained from end users are recorded
- Control international cross border data transfers through Binding Corporate Rules (BCR)

Conditions for consent

Impelsys

- Unambiguous
- No pre-ticked boxes
- Freely given
- Withdrawal
- Transparency
- Management

Refer Consent Procedure

- Consent must be obtained through clear **affirmative** action.
- Obtain Consent at the time of first interaction or explicitly
- At the time obtaining consent highlight about their right to withdrawing of consent.
- End user or data subject can **withdraw** the consent at any time. Provide an option to withdraw the consent or monitor privacyoffice@impelsys.com for withdraw consent requests.
- **Stop** the processing after approving and closing of withdrawal consent.

Record Data Processing

what type of personal data is collected and/or processed

category of data

purpose of processing

processing agreements or contracts,

sub-processing or third-party,

recipients of data,

any transfer to third country,

security techniques and measures applied,

safe-guard controls,

storage and retention, disposal details

Refer Data processing register, data processing questionnaires

- DPR responsible for his/her functional team should read data processing questioner first.
- Fill the data processing register at data or data set level in every product, project, service delivery etc.,
- DPRs can adopt these methods to fill the register - interview with key resources, validate the existing documents, filling the questionnaire etc.,
- Review the filled processing register and document it

Data Privacy Impact Assessment

Impelsys

Objective: To minimize the privacy risks

Set criteria for conducting DPIA

Privacy impact criteria

Periodic re-assessment

Refer DPIA process and template. Refer Risk Register and treatment plan template

- Conduct DPIA as per conducting criteria to identify the privacy risks.
- Assess the risk based on risk score = Impact * likelihood as accept, transfer, terminate, mitigate.
- Record risks in risk register, assign owner and monitor
- Establish and apply controls –
  - **legal** controls,
  - **security** controls,
  - **technical** controls,
  - **logical** or **physical** security controls,
  - organizational controls
  - Risk on cloud computing and **cloud** controls

Privacy by design and default

Impelsys

Proactive not reactive

Respect for user privacy

Visibility and transparency

Compliance to GDPR

- Principles
  - Proactive and not reactive
  - Embedded into design
  - End to end security
  - Respect for user privacy
  - Privacy by default setting
  - Full functionality
  - Visibility & transparency
- Methods
  - Data minimization be default.
  - Process and store data only if and as longs as needed
- Benefits
  - Reduces the cost
  - Efficient development
  - Compliance to GDPR
  - Additional sales pitch in business due to greater privacy

Breach (Violation of GDPR)

Impelsys

Violation of GDPR principles

Data Processor notifies breach to – DPO, controller, supervisory authority (if applicable) and data subject.

Refer breach management procedure, breach register and notification template

- What is breach
  - Compromise of processing, Unwanted modification of personal data
  - Disappearance of personal data, Excessive collection of personal data
  - Unauthorized or inappropriate linking of data, Failure to address the rights of data subject
  - Processing of PII without the knowledge or consent of the PII principal
  - sharing or repurposing PII with third parties without the consent of PII principal
  - unnecessary prolonged retention of PII
- What to do
  - Controller without undue delay, not later than 72 hours should inform to controller / SA - impact, measure taken to address. Inform to Data subjects.
  - Address the breach. Correction or corrective action (design??), Re-assess Risk and strengthen security control & measures.
  - Document the breach. SA can verify the compliance of breach at any time.

Impelsys

Data Subjects Rights

Rights of data subjects

GDPR has given more power or control to data subjects over their personal data - Rights

- Right to be informed
- Right of access
- Right of rectification
- Right to erasure ('right to be forgotten')
- Right to restrict the processing
- Right of data portability
- Right to object
- Rights related to **automated decision making** including profiling
- Transparency, Communication and Modalities

Refer Data Subject Rights Procedure and Guidelines

Rights to be informed

- We need to provide '5 W' information to the data subjects if their personal data is collected.
  - Who – The identity and contact details of controller, the data protection officer contact details, to whom data is shared
  - What – What data is collected and what purpose data is processed.
  - Why – Why the data processing is necessary ie legal basis of processing
  - Where – Where the data is stored, any international transfers or sharing
  - When – How along data is stored and when it will be disposed.
  - How – How the data subjects use their rights

- What/How we should do:
  - Define inform mode: Eg: Policy
  - Inform at the time of first consent ie collection etc.,

What does it mean?

What we should do?

Rights of Access

- Data subjects that you hold information about will now have the right to ask/access about their personal information :
  - What information you hold about them?
  - Why you hold it? Purpose of processing;
  - How long you've had it?
  - How long you intend to hold it
  - What you intend to do with it and
  - Ensure that data held about them is accurate.
  - To whom data have been disclosed, any third party or third country
- What/How we should do?

- Either provide an option to ask through web or any other electronic form or send an email to privacyoffice@impelsys.com
- Define mode of asking in policy or consent.
- **Acknowledge** within defined TAT.
- **Address** within defined TAT ie a month.

What does it mean?

What we should do?

Rights of Rectification

- If the data subject from whom you have collected & processed their personal information, finds out that you hold incorrect data on them
  - They have the right to contact you.

- What/How we should do?

  - Either provide an option to ask through web or any other electronic form or send an email to privacyoffice@impelsys.com
  - Acknowledge within defined TAT.
  - Correct the data without undue delay ie defined TAT.
  - Respond & confirm the update through statement/email.

What does it mean?

What we should do?

Right of ERASURE

('right to be forgotten')

Impelsys

- Data subject has right to ask for erasing their data
  - They have the right to contact you.
- What/How we should do?

  - Either provide an option to ask through web or any other electronic form or send an email to privacyoffice@impelsys.com
  - **Acknowledge** within defined TAT.
  - Fully **identify** the data subject
  - **Check** –
    - Is there any legal basis to continue to store/process the data
    - If data subject has withdrawn the request
  - **Erase** –
    - Primary storage, backup storage, achieve storage, cloud storage etc.,
  - **Respond** back along with 'reasonable effort' have been made in deleting all the data.

What does it mean?

What we should do?

Right to Data Portability

- Data subject has the right to receive or have transmitted to another in a structured and machine readable format.
  - They have the right to contact you.

- What/How we should do?

  - Either provide an option to ask through web or any other electronic form or send an email to privacyoffice@impelsys.com
  - **Acknowledge** within defined TAT.
  - Fully **identify** the data subject
  - **Check** –
    - Is data subject has given the consent
    - Processing is necessary on basis of contract, legal, legitimate interest
  - **Provide a** copy in machine readable format or export to specified another

    Within a defined TAT or a month
  - If exported – **remove** from the all internal systems

What does it mean?

What we should do?

Right to Restriction of processing

- Data subject has the right to restrict from being processed until they will gave consent again
  - They have the right to contact you.

- What/How we should do?

  - Either provide an option to ask through web or any other electronic form or send an email to privacyoffice@impelsys.com
  - **Acknowledge** within defined TAT.
  - Fully **identify** the data subject
  - **Check** –
    - Is data subject has given the consent
    - Processing is necessary on basis of contract, legal, legitimate interest
  - **Suspend processing,** respond to the request
  - **Reject and Continue the processing** – justify with proper reason.

This will be validated by supervisory authority in case data subject file a complaint.

What does it mean?

What we should do?

IMPELSYS PRIVACY OFFICE

If you have any questions about PIMS and/or GDPR, please reach out to privacyoffice@impelsys.com.

Please visit www.impelsys.com/gdpr to know more on our getting ready for GDPR.