EURADOS Report 2026-02
Oberschleißheim, April 2026

EURADOS
European Radiation Dosimetry Group e. V.

Dosimetry and Information Technology

Robert Bernat, Panagiotis Askounis, Vedran Bandalo, Codrut Cherestes, Nicky Gibbens, Carolina Hernandez Gonzalez, Irene Mas, Anatol Oprea, Begoña Perez Lopez, Samy Keymis

ISSN 2226-8057
ISBN 978-3-943701-43-2
DOI 10.12768/3185-R132

European Radiation Dosimetry Group e. V.

EURADOS Report 2026-02

Oberschleißheim, April 2026

Dosimetry and Information Technology

Robert Bernat[1], Panagiotis Askounis[2], Vedran Bandalo[3], Codrut Cherestes[4], Nicky Gibbens[5], Carolina Hernandez Gonzalez[6], Irene Mas[7], Anatol Oprea[4], Begoña Perez Lopez[6], Samy Keymis[8]

[1] Ruđer Bošković Institute, Zagreb, Croatia

[2] Greek Atomic Energy Commission, Athens, Greece

[3] Mirion Technologies (AWST) GmbH, Munich, Germany

[4] Dositracker SRL , Măgurele, Romania

[5] UK Health Security Agency, Oxford, United Kingdom

[6] Centre for Energy, Environmental and Technological Research (CIEMAT), Madrid, Spain

[7] Centro Nacional de Dosimetría, Valencia, Spain

[8] Vinçotte, Vilvoorde, Belgium

ISSN 2226-8057

ISBN 978-3-943701-43-2

DOI 10.12768/3185-R132

Imprint

Issued by:
European Radiation Dosimetry Group e. V.
Ingolstädter Landstraße 1
85764 Oberschleißheim
Germany
office@eurados.org
www.eurados.org

The European Radiation Dosimetry Group e.V. is a non-profit organization promoting research and development and European cooperation in the field of the dosimetry of ionizing radiation. It is registered in the Register of Associations (Amtsgericht München, registry number VR 207982) and certified to be of non-profit character (Finanzamt München, notification from 2025-01-31).

Liability Disclaimer

Content:

Abstract

This report is aimed at Individual Monitoring Service's (IMS) staff who have limited background in Information Technology (IT) to provide guidance and advise on data management and security.

Data security and practice has regularly been raised at EURADOS Working group 2: Harmonization of Individual Monitoring in Europe plenary meetings. Due to increasing interest in this area, a task group on Dosimetry and Information Technology was formed in 2020.

The increasing interest among IMSs results from number of factors.

- For some time, there has been a trend towards communicating with clients electronically, for example by e-mail or by online access/ customer extranets. This is true in all aspects of life, from banking and medical records to social media.
- As criminal activities have become more sophisticated, there has been an increased need to make all communications secure, and individual monitoring of ionising radiation is no exception.
- With the modern reliance on electronic records, there is a greater need for reliability and for protection against degradation.
- Legislation such as the European General Data Protection Regulation places obligations on all data owners and data processors. The obligations include, for example, a "right to be forgotten" – the discarding of data that is not legitimately required.
- Increasing focus on quality accreditation that requires all records to be kept reliably.

For IMSs there is a need to balance the various requirements for long-term retention, secure transmission and discarding of obsolete data. Because IMSs have different contexts (service size, nature of organisation, national requirements) the principles may need to be interpreted differently. The present work seeks to provide advice to support that.

Dosimetry and Information Technology is a broad topic, and the intention is that work will focus on various issues in turn. Topics covered in this report have been chosen according to their importance.

Glossary

Abbreviation	Word / Phrase	Definition
2FA	Two-factor authentication	Electronic authentication method in which a user is granted access to a website or application only after successfully presenting two pieces of evidence to an authentication mechanism.
API	Application Programming Interface	Connection between computers or between computer programs.
CIFS	Common Internet File System	Network file-sharing protocol that allows applications to read and write to files and request services from file servers over a network.
DAS	Direct Attached Storage	Digital storage directly attached to the computer.
DZM	Demilitarised Zone	A physical or logical subnetwork that separates a local area network from untrusted external networks (such as the internet). It is used to host services that require external access while limiting direct exposure of the internal network.
EDPB	European Data Protection Board	Independent European body, which contributes to the consistent application of data protection rules.
GDPR	General Data Protection Regulation	A regulation that governs the processing of personal data of individuals and requires that such processing be lawful, fair, and transparent.
HDD	Hard Disk Drive	Electro-mechanical data storage device that stores and retrieves digital data.
IMS	Individual Monitoring Service	Radiation *Monitoring Service that* monitors ionising radiation exposure to individual workers.
IAPP	The International Association of Privacy Professionals	A non-profit *association* with a mission to define, promote and improve the *privacy* profession globally.
IT	Information Technology	A branch of computer science, defined as the study of procedures, structures, and the processing of various types of data.
LAN	Local Area Network	A network that connects computers and other devices within a limited geographic area, such as a building or laboratory, enabling internal communication and resource sharing.

Abbreviation	Word / Phrase	Definition
NAS	Network Attached Storage	File-level computer data storage server connected to a computer network providing data access.
NDR	National Dose Registry	Registry that contains the dose records of individuals who are monitored for occupational exposures to ionizing radiation.
NFS	Network File System	Network file sharing protocol that defines the way files are stored and retrieved from storage devices across networks.
OS	Operating System	System software that manages computer hardware and software resources and provides common services for computer programs.
RAID	Redundant Array of Inexpensive Disks	Method that combines multiple physical disks into a single logical unit.
SAN	Storage Area Network	Computer network which provides access to consolidated, block-level data storage.
SATA	Serial Advanced Technology Attachment	Command and transport protocol that defines how data is transferred between a computer's motherboard and mass storage devices.
SCSI	Small Computer System Interface	Electronic interface that enables PCs and servers to communicate with peripheral hardware.
SMB	Small to Medium Size Businesses	Businesses whose personnel and revenue numbers fall below certain limits (EU: < 250 employees and annual turnover ≤ € 50 m).
SSD	Solid-State-Drive	A storage device that uses flash memory and integrated circuits instead of mechanical components.
SSO	Single-Sign-On	Authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials.
TOTP	Time-based One-Time Password	Type of one-time password that uses the current time as a source of uniqueness.
U2F	Universal Two Factor Authentication	Open standard that allows you to use a physical security key for two-factor authentication.
VPN	Virtual Private Network	Network architecture for virtually extending a private network across one or multiple other networks which are either untrusted or need to be isolated.

1. Data Storage and Network Segmentation

Data is a collection of discrete values that conveys information, describing quantity, quality, fact, statistics, other basic units of meaning, or simply sequences of symbols that may be further interpreted. Within an organisation, there are a number of ways in which your data is likely to be stored. However, it may not always be clear which data resides where. The expansion of digital services and communication tools mean that files are constantly being shared across locations and uploaded to different platforms, creating a lengthy digital paper trail. Data can be stored locally, on the device you are using, or over the network.

Storage of the collected information (both data on customers and their dose results) must insure up-time/data availability, integrity of data, and security. We will briefly go through each of these in the following sub-chapters together with some recommendations. Uptime only measures the total time that a system is available, while availability considers factors that may impact the system's performance. Data integrity is the accuracy, completeness, and quality of the data as it's maintained over time. Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access.

1.1 Data availability

Data availability can be split up into two related, but different, concepts: **up-time/redundancy, and backup**.

Up-time/redundancy deals with how to ensure that data stays available in day-to-day routine operations, that is, the use of techniques like Redundant Array of Inexpensive Disks (RAID) and/or failover to increase tolerance of equipment failure. It is critical to understand that redundancy is not backup.

Backups are NOT up-time improving technology but a last resort in case of massive failure of routine systems. This also means that they must be on a completely separate system from the normal running system. It is especially important that access control is different between routine and backup systems to ensure that compromise of one does not affect the other. By having separate system access, control backups can be protected during increasingly more common (crypto) ransomware attacks.

1.2 Integrity of data

With the advance of new technology like Solid-State-Drives (SSD) and new requirements in ISO/IEC standards, data integrity is becoming more important. In general, the integrity of data is split into **Protection against unintended change** (failure of equipment, interference with the equipment and so on) and **Protection against intended change** (limiting access to only necessary, logging of all data changes irrespective of access level).

Protecting data against unintentional change is fairly limited with only a few techniques available at this time. This normally involves the use of Redundant Array of Independent Disks (RAID) or similar techniques as it can check the data and repair it. The goal is to be able to detect and then repair (either on the fly or from backups) any data corruption. This is especially important if SSDs are used for long term storage, as data retention times are far shorter (and more sensitive to influences like cosmic radiation and storage temperature) than for the Hard Disk Drives (HDD).

Protecting against intentional changes is more difficult as the majority of computer systems allow administrators full control. Common approaches are to limit the access to data (read only access rather than full access) and/or to have the sensitive data cryptographically signed (key kept secure and not accessible to people with access to the storage system) so that any changes (intentional or unintentional) can be detected (it's only detection, there is no provision for recovery of corrupt data in this case) [1].

1.3 Backup

Backup should be considered a last-resort option for recovery of data. This means that backups must be made often enough (how often depends on the data production timing) to ensure that all data, that is not recoverable by other means (e.g. by measuring the dosimeter again), is available in case of failure of the primary systems.

Restoration of backups should be regularly checked to confirm that everything works as intended, and that backups cover all the data needed. While this is additional work, it ensures that if the primary system goes down there is a way back. Test recovery can also be seen as recurring training in the recovery process that will speed up recovery when needed for real.

It is critical to have separate access control for primary systems and backups. The same set of credentials should never work on both systems so that compromise of one does not affect the other. This is becoming more important with advanced threats like ransomware that can easily encrypt backups too. Optimally, completely separate access controls and use of hardware 2-factor authentication should be implemented.

1.4 General network design

With the current threat landscape leaning towards, *when* an organisation will be hacked/ attacked, rather than *if*, the design of the network should tend towards minimising the damage from any breach. This, in general, means segmenting the network into protected enclaves that have minimal, if any, contact with each other. However, segmentation introduces a degree of inconvenience, so there will always be a balance between security and ease of use. For each system, there should be evaluation of potential consequences if compromised versus the day to day ease of use.

Figure 1. shows a very simplified segmented network with following components:

- Office network
  - Network for normal users, with access to internet
  - Sealed off from other networks/systems except for users who must have access
- Production network
  - System critical, responsible for dose reads
  - Fully sealed off network that has one-way communication to the dose management system (dose data export)
  - Separate credentials from any other system, preferably backed by 2-factor authentication (2FU) using hardware Time-based one-time password (TOTP)
- Dose management system
  - System critical, responsible for pairing of personal data and dose results as well as issuing dose reports to customers
  - Due to the need for communication this system cannot be sealed off completely
    - It needs input from the production system (doses)

        - It needs input from customer support in the office network
        - It needs the ability to export all this data to a "customer access" portal
    - Firewalled on all sides with only absolutely necessary services allowed through
    - Separate credentials compared to other networks and backed by 2-factor authentication using hardware or TOTP
- Customer access
    - High value system that is exposed to the internet for customer access
        - Exposure to internet is always dangerous as it demands very rapid response to any identified vulnerabilities in the software used which leads to high workload
        - Large, exposed attack surface if direct access to web/application/similar service is exposed
    - Must be able to communicate with the main dose management system
        - User must be able to change some of the data
    - Should use separate system and credentials from the dose management system
    - 2-factor authentication (hardware or TOTP) should be used both by customers and administrators (In general all administrative tasks should demand 2-factor authentication)

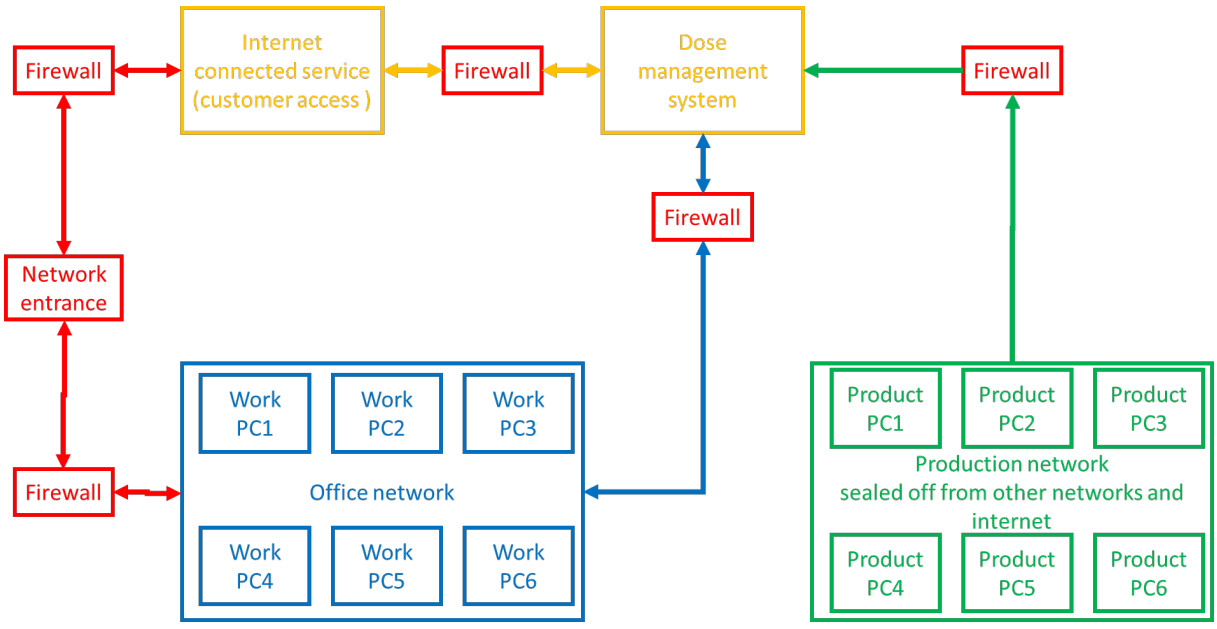

Figure 1. Simplified schematic of a segmented network designed to protect most critical systems

Even the simplified schematic shows that there are several critical systems and that there is a significant amount of work in securing them. In the interest of simplification, redundancy and backup are not mentioned here. However, they are an integral part of the network and, , backups, in particular, should be decentralized just like the systems/networks they are protecting (see Figure 2.). This approach, together with separate access credentials for backups, increases the chance that a compromised system be protected from an attack over the entire network and all the backups. The primary goal is to minimize impact from a breach, which could as there are no perfectly secure systems.

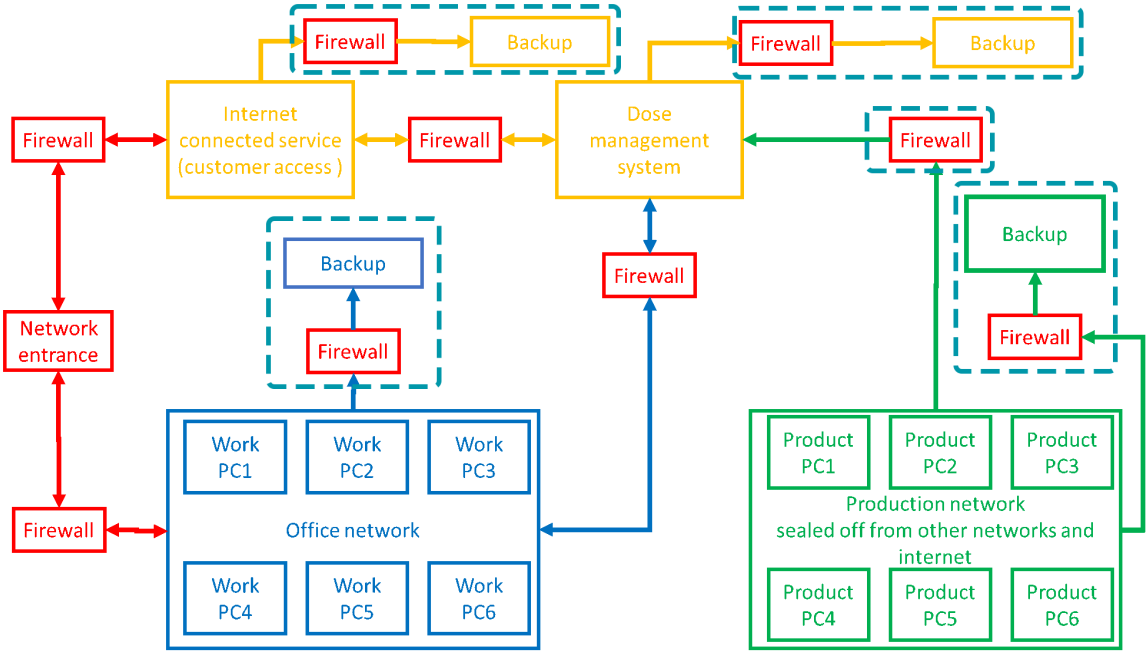

Figure 2. Simplified schematic of a segmented network designed to protect most critical systems

1.5 Data storage scaling

Scalability is a critical factor in data storage, particularly in the modern business landscape where data volumes are growing at an exponential rate. A scalable storage system allows for the accommodation of increasing data loads without compromising performance or efficiency. It is a forward-looking strategy, ensuring a system can handle future data growth and demand. Scalability is not just about capacity, but also about performance. As data volumes increase, businesses need a system that can quickly process and retrieve data. Data storage requirements vary for each IMS, depending on the size of the laboratory, the number of monitored workers, and the data retention period.

1.5.1 Direct Attached Storage (DAS)

DAS is a storage that is **directly attached to a computer** without using a network. DAS (Direct Attached Storage) is storage that is directly connected to a computer without using a network. It can consist of one or more internal drives, such as traditional HDDs or faster SSDs, typically connected via a Serial Advanced Technology Attachment (SATA) interface. DAS can also include external devices containing multiple drives, connected through high-speed interfaces such as Small Computer System Interface (SCSI) [2].

DAS is a storage solution that is meant for small to medium size business (SMB). An example of definition of SMB is shown in Table 1.

Table 1. An example of definition of SMB in the EU. Source: https://www.destatis.de

Size class	Persons employed	Annual turnover
Micro-enterprises	Up to 9	Up to EUR 2 million
Small enterprises	9-49	EUR 2-10 million
Medium-sized enterprises	49-249	EUR 10-50 million
Large enterprises	More than 249	More than EUR 50 million

☺ The main advantages of DAS are that it is high-performing, simpler to setup and configure, and the least expensive approach for small storage requirements.

☹ It cannot be managed over a network and may not have the same level of redundancy as a NAS or SAN. If any component fails on the server and stops the application, access to the data will also be lost. Another challenge of DAS is the likelihood of running out of space. A direct attached solution does not scale well.

1.5.2 Network Attached Storage (NAS)

A NAS system consists of **specialized file servers** that are set up, built or designed specifically for the purpose of sharing files over a network using a network protocol, such as NFS. A NAS refers to storage elements that connect to a network and provide file access services to computer systems. A NAS element consists of an engine that implements the file services (by using access protocols, such as NFS or CIFS) and one or more devices, on which data is stored. A NAS element might be attached to any type of network. A NAS can be seen as a network drive (via Ethernet) and as such, it can be used to save documents and files as well as read them. Fundamentally, a NAS is a computer, optimized in hardware and software, to be a file server [3].

☺ NAS is ideal for small to medium sized businesses because it allows a cost-effective way to gain data access for multiple clients, quickly, at the file level. SMBs can gain from its performance and increase their productivity. A few other advantages include, easy setup and configuration compared to SAN, maximum storage resource utilization, better physical resilience (compared to DAS) and the easy-to-provide RAID redundancy to a large number of users.

☹ Latency issues due to network issues.

1.5.3 Storage Area Networks (SAN)

As defined in the IBM's Redbook, "Introduction to Storage Area Networks", a storage area network (SAN) is a **complex and specialized high-speed network** which has a main purpose of transferring data between computers and storage devices. Even though SANs have originally used high-cost fibre-optic cabling for network connections, nowadays technological developments allow the use of lower cost copper wiring-based solutions and equipment such as Gigabit Ethernet. A SAN typically has direct connections to all devices on it, which allows for, server to server, server to storage and

storage to storage high-speed communication, even if SAN storage devices and servers are located far away from each other [4].

☺ Ability to transfer large data blocks. This is very useful for bandwidth-intensive applications such as imaging, database (cloud computing, virtual environments), and transaction processing. Also, SAN offers complete reliability and 24/7 availability of data. SAN is limited to the enterprise sector since a large investment is required for its design, development, and deployment. Additionally, because a SAN could span a distant location containing a secondary storage array, SAN also enables more effective disaster recovery processes.

☹ Cost: limits their useto the enterprise sector since a large investment is required for its design, development, and deployment

Simplified schematic of different scales of storage systems is shown in Figure 3.

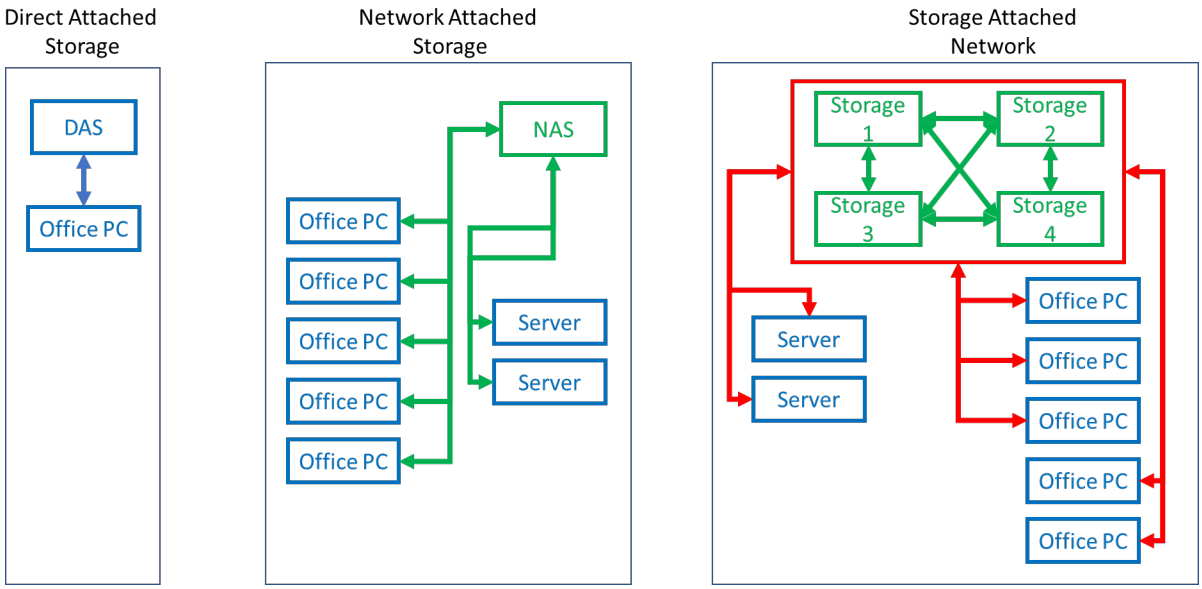

Figure 3. Simplified schematic of different scales of storage systems. Starting with DAS where storage is attached directly to a specific computer, NAS where storage is exposed to the network of computers and server, to SAN where storage is built-up as a network allowing for direct data transfer between storage units without having to transfer data past an operator (PC or a server)

1.5.4 Cloud Storage

Cloud storage can be described as a service model in which data is transmitted, stored and maintained remotely on off-site storage systems. The stored data is made available through a collocated cloud computing service, a web service Application Programming Interface (API), or through applications that use the API (such as cloud desktop storage, a cloud storage gateway, or web-based content management systems). For Cloud storage, users pay monthly to cloud storage providers depending on their consumption rates [2,5–8].

☺ There is no need to invest any capital on storage devices, no need for technical expertise to maintain the storage, backup, and replication; plus importantly it helps disaster management and collaborative working style instead of individual work by allowing others to access shared data

☹ Performance and Security concerns. Access to cloud data is limited by network throughput and latency. Despite improvements in internet performance, cloud access is still poor in comparison to local network storage. Data security is the biggest issue with cloud storage. Cloud storage means handing over the control of confidential information to a third-party company. Experts agree that using encryption on all data stored in a cloud is essential, although depending on the application, this is easier said than done.

Finally, it should be noted that use of cloud or even dedicated hosting has some serious implications with respect to GDPR [9] and should beused only after careful consideration of the CJEU court decision in 2018 [10] and opinions of the EDPB. In effect, it means that using any US-based service is not acceptable, even if servers are in EU.The US law (FISA and Cloud Act) puts demands on administrators based in US to provide any data they have access to, irrespective of where this data is located. Due to these issues, it is safest to use services that only have presence in the EU as they will not be impacted by laws outside of the EU.

2 Safe and Effective Communication Paths and Safe and Effective Data Transfer

This chapter will cover communication paths, types of data exchange records, possibilities of encryption, segmentation, data portability and recommendations for Individual Monitoring Services.

Data communication is the process of transferring data from one place to another or between two locations. It allows paper documents, electronic and digital data to move between two locations, no matter where the two are located geographically, what the data contains, or what format they are in.

The type of data transmission demonstrates the direction in which the data moves between the sender and receiver.

- **Simplex data transmission:** Data is sent from sender to receiver
- **Half-duplex data transmission:** Data can transmit both ways, but not simultaneously
- **Full-duplex data transmission:** Data can transmit both ways at the same time

Prioritizing safe and effective communication and data transfer is fundamental to ensuring regulatory compliance and maintaining the integrity and reliability of Individual Monitoring Services. The importance of accuracy, confidentiality, and efficiency will be assured by implementing robust communication strategies and secure data transfer methods.

2.1 Types of Communication paths used by Individual Monitoring Services

Voice based communication. Eg. Direct communication between IMS and customer related to problems with a specific problem or with National Regulator	
☺	Allows for real time communication, enabling quick clarification and decision-making. Efficient for complex issues. Effective for discussing complex topics that require back-and-forth dialogue. Accessible and easy to use. Most people are familiar with making phone calls
☹	Phone conversations don't provide records, making it hard to reference later, and may generate potential mis-communication. Security Risks: Conversations can be intercepted. Special caution if sensitive information is discussed. The identities of the communicating parties are not properly verified. Time Constraints: Calls can be time-consuming, and finding mutually available times can be challenging.

Paper based communication. Eg. Filled in forms sent by the costumer to the IMS to apply for different type of service, different type of dose report sent to the customer, administrative communication with customer.	
☺	Control Over Recipients: Easy to *control* who the information goes to Formality: Postal communication can be perceived as more formal and professional. Easy to use: most people are familiar with sending a postal mail. Automation: Reports or notices can be easily automated for distribution to a designated list of recipients.
☹	Economic and environmental costs derived from printing and postal delivery Delivery time: Letters can take days or weeks to arrive, affecting the speed of communication. Leaves no or little records, depending on the courier.

Digital based communication. Eg. Encrypted emails related with dose incidences, logistics of dosimeters, web portal access to send dose records to the National Dose Registry, web portal access to customers to access to different IMS services and data..	
☺	Record-keeping and traceability: Provides records of data access and exchanges, facilitating audits and tracking Remote accessibility allows systems to be accessed from anywhere with an internet connection, supporting remote working and greater flexibility. Authentication and security: Enables the implementation of authentication methods (passwords, biometrics, tokens, data encryption etc.), enhancing information protection. Speed and efficiency: Messages are delivered in real-time, reducing waiting times compared to postal mail.
☹	High initial costs: Implementing digital systems can require significant investment in infrastructure, software, and training. Risk of Cyberattacks and technological dependence: Digital communication is vulnerable to data breaches and malicious hacker attacks that may compromise security and privacy.

2.2 Types of Data exchange Records involved

Different types of data records may be classified according to:

- Personal data not including dose data.
  - Customer contact data used for administrative tasks (invoices, etc.) or logistic issues (sending dosimeters by post)
  - User/occupational worker personal data used to manage dose records
  - Statistical graphs of data not related with doses and non-identifiable graphs
- Dose data
  - Dose data transferred to internal or external storage
  - Dose data sent to customer (Monthly/ annual dose reports /individual dose report or dose history)
  - Dose modifications sent by customer to IMS
  - Dose data sent to regulator and/or national dose registry
  - Dose data sent to Occupational Health Physician or Radiation Protection Physician.
- Non personal data
  - Eg. anonymized data
  - Eg. notes, news and announcements from IMS to the customers

Different levels of security should be established according to the criticality of the data involved.

With respect to Dose data, in every country National Regulators will establish if dosimetric data shall be considered as health data and catalogued as "Sensitive Personal data", or not ("Personal Data") for GDPR purposes.

2.3 Data encryption

Data encryption converts data from a readable, plaintext format into an unreadable, encoded format. Users and processes can only read, and process encrypted data after it is decrypted. The decryption key is secret, so it must be protected against unauthorized access.

Encryption is the process of converting data into an unusable form and does not itself stop hacking or data theft. Instead, it prevents stolen content from being used, since the hacker or thief cannot see it in a plaintext format.

- **Use encryption where possible**. Dosimetry data may be personal, medical or commercial in nature and must therefore be handled confidentially. By default, IMS's should send data in encrypted or other protected format; however, the needs of the client must be taken into account. Different arrangements may need to be made for clients whose technology restricts or controls incoming data, or who prefer to receive hard copy documents.
- **Engage IT support**. If your service is part of a larger organisation, collaborate with your IT support team in order to make your encryption system efficient and effective.

- **Choose an easy-to-use encryption system**. Your clients do not want to waste time extracting data from complicated systems. Remember they may not have much IT expertise at their disposal. Aim for a system that balances information security with ease of use.
- **Engage with the clients**. The transmission of encrypted data is a two-ended process. Some clients' IT infrastructure may restrict, for example, the downloading of software. Find out what these restrictions are before commissioning an encryption system.
- **Provide information and help**. Clients may need help in learning how to use encryption. Provide simple written instructions, and make telephone help available.
- **Decide what needs encrypting**. Does the client require all communications to be encrypted, or only some? For example, it is likely that all dosimetry reports will need to be encrypted, but what about general letters, newsletters etc?
- **Give plenty of notice**. When commissioning a new encryption system – whether introducing one for the first time or switching to a different one – give clients at least three months' notice.
- **Have a fall-back option**. If the client has a problem – whether short- or long-term – in accepting encrypted e-mails, they still need to receive their dosimetry reports. Ensure that you have at least one way of sending the reports outside of an encryption system. Examples might be to use a zipped, password-protected file

Have a time limit on links. If an e-mail contains a link, which the client needs to follow, it will improve security if the link expires after a certain time, e.g. 28 days.

2.4 Recommendations for Individual Monitoring Services

IMS's should ensure that data is accessible, consistent and protected.

IMS's should identify effective communication channels according to the user type without putting aside security considerations.

Two main security aspects need to be considered when dealing with personal and/or sensitive data:

1. Identification of the recipient /authentication to achieve data integrity
2. Channel security: needed to achieve confidentiality and protect data from disclosure

	Authentication of recipient	Security in the channel
Voice based communication	+	+
Paper based communication	++	++
Digital based communication	+++	+++

Only digital based communication may provide these two aspects with guarantee. However, several issues need to be taken into account when considering digital based communication.

2.4.1 Recommendations for Digital based communication

SMB's would need to put a medium term plan in place (3-5-year plan) to implement this approach. SMB's must integrate both traditional and digital channels to meet diverse customer preferences effectively. Relying solely on traditional methods may overlook the efficiency and reach of digital platforms, while an exclusive focus on digital can miss the personal touch of traditional methods. The plan would need to include consideration of costs (products, support and maintenance).

Digital based communication, if correctly implemented, offers: flexibility, accessibility, traceability, immediacy, and many more advantages. Therefore, an IMS should consider transition to digital based communication.

General purpose IT security measures:

- Corporate IT System Security Accreditation:
  - Ensure compliance with recognized security standards (e.g., ISO 27001, NIST).
- Conduct external audits to validate adherence to security policies
- User training
  - Implement ongoing training programs on cybersecurity threats and best practices.
  - Conduct phishing simulation exercises to evaluate employee responses.
- Carefully designed internal network infrastructure and firewalls.
  - Utilize network segmentation to limit lateral movement of attackers.
  - Configure firewalls with strict inbound and outbound policies.
- Internal segregated network.
  - Implement VLANs to separate different types of traffic based on sensitivity.
  - Control access to the segregated network through robust authentication.
- Authentication of all electronic data transfers
  - Use digital signatures to ensure data integrity and authenticity.
  - Require Multi Factor Authentification (MFA) for access to email accounts and communication platforms.
  - Use strong password policies
  - Implement Identity and Access Management (IAM) solutions to control access.
- Access control:
  - Implement role- based access control (RBAC)
  - Regularly audit access permission to sensitive information
- Encryption to prevent access to intercepted information (see 2.3).
- Secure channels for electronic data transfer:
  - Require secure protocols for all data transfers (e.g., VPN, HTTPS, SSH).
  - Disable insecure data transfer methods (e.g., unencrypted FTP).
- Logging and monitoring of access
  - Use a Security Information and Event Management (SIEM) system for logging analysis.
  - Establish alerts for unauthorized or unusual access attempts.
- Protocols for data breach response
  - Develop an incident response plan that includes internal and external communication.
  - Establish a dedicated incident response team with defined roles and responsibilities.
- Risk analysis
  - Conduct regular risk assessments to identify vulnerabilities.
  - Prioritize remediation based on potential impact.
- Use security software:
  - Implement antivirus and anti malware solutions on all devices
  - Keep regular software and application updates to fix vulnerabilities.
- Vendor and Third-Party Review:
  - Evaluate the security of vendors and partners before data sharing.
  - Establish security clauses in contracts with third parties.

- Potentially sign a Non-disclosure Agreement (NDA)

Web portals:

- Web server maintenance support that includes security updates at system, application and software level.
- Web server architecture: Since web servers need external access, it should also be set in a separate DMZ subnetwork ("demilitarized zone": a physical or logical subnet that separates a local area network (LAN) from other untrusted networks).
- Use encryption provided by HTTPS, instead of completely unencrypted HTTP.
- Authorisation:
  - Only previously authorized users can access. Keep records of authorization forms.
  - Only nominal (not generic) users allowed.
  - Accept GDPR and user responsibility on first access.
  - Carefully design authorizations by using hierarchy trees and type of data access to the platform
    - Role-based Access Control: i.e. read access vs read and modify authorization, access to basic data vs access to all data including sensitive data… etc.
    - Restrict access to data from other institutions
- Authentication:
  - Access control: User/password plus multifactor authentication (TOTP or hardware key like U2F)
  - If digital signature used (i.e. to send customer application forms), validation of digital signatures shall be considered
- Data Privacy:
  - Data restriction: Each user should only be able to access data from his own institution
  - Data anonymization. Consider only including the IDs of dosimeters, if the client has the list of correlations on their side.
- Options to improve more efficient communication:
  - Provide email message, SMS/IM app message if any relevant not sensitive data is available for the user.
  - Include digital application forms including digital signature to request IMS services (new hospital, service or dosimeter user registration, ..)

Emails:

- Use Secure/Multipurpose Internet Mail Extensions (S/MIME) or Pretty Good Privacy / GNU Privacy Guard (PGP/GPG) encryption whenever personal data are involved. This is the only secure way to transfer sensitive data by email; however, it is not straightforward to implement.
- Other less secure options may include ciphering the content of the email with a previously agreed password using some external tool like ZIP compression.

Cloud servers:

- Cloud storage protects against the loss of sensitive data via strong backup and data recovery services.
- However the security of uploading relevant data in the cloud, generally managed by an external/private company, may become a major concern, since you entrust the security of

your data to that company. Security compliance accreditation of the data storage service provided should be required and provided.

VPN access /Remote office network configuration:

- Provides encrypted communication to internal IMS network
- Provides secure options to work online

2.4.2 Recommendations for Paper based communication

Postal mail has been traditionally used by IMS to:

- Send periodic dose reports to the customer
- Send overdose notifications
- Send dosimeter inventory in a shipment

Overdose notifications, as well as periodic dose reports are usually a legal requirement in most countries. Therefore, many IMS chose to perform these reports by postal mail in order to automate and ensure that the information is always delivered and legal requirements are fulfilled. These notifications are delivered by postal mail to the postal address provided by the client.

The destination postal directions should be fully specified (including the complete Name and address instead of a job title).

Personal data included in the message **should be restricted to the minimum necessary** (i.e. using unique identifier code, instead of personal data of the user, if the client has the correspondence of each ID with the user pseudo-anonymised).

With regard to providing a safe and effective service, it is highly recommended to agree by contract with the carrier on

- The maximum time lapse for the delivery.
- Number of tries to deliver and place of delivery
- Tracking of the delivery.
- Return if non-deliverable

2.4.3 Recommendations for Voice based communication

However, in a few particular cases, using the phone might be quicker to resolve time-sensitive incidences, and is a more effective means of communication. In these cases:

- The consignee should be identified to the IMS prior to the information exchange (Recommended to check the consignee requiring some personal information, or private code shared in the web, …)
- Personal data should be avoided in the conversation. A unique code identifying the dose history may be used.

2.5 Segmentation

Data Segmentation is the process of dividing a large dataset into smaller, more manageable segments based on specific criteria or characteristics. Effective segmentation can be a turning point for businesses looking to enhance their existing customer data and analytics to better understand their customer requirements.

To implement the right kind of Data Segmentation and to communicate more effectively, key strategies include:

- User access only to necessary areas/systems
- Segment logins (avoid SSO where single compromised password gives access to everything)
- Hardware 2-factor authentication
- Segment networks
    - Keep production systems sealed off from the rest of the network with separate access controls
        - Sealed network does not need to track OS updates and thus there is a lower risk of interruption due to changes to the underlying OS. In this case the security of the system depends fully on the isolation, as over time more and more security relevant bugs will be discovered and readily available for abuse by anyone who gains access to the network
    - Ransomware (an automated attack that encrypts all accessible data, making it inaccessible to the user). Effective protection includes network segmentation and backup.
- Backups
    - Ensure that backups are one way and that system backing up cannot corrupt older backups.

2.5.1 External access / services

- Minimise attack surface (expose VPN rather than application server)
- Encryption (VPN, TLS depending on service/application)
- Secure authentication for remote work (hardware keys or TOTP rather than just passwords)
- Segment authentication (avoid single set of credentials giving access to everything)
- Minimise access to only needed data/services
- E-mail training (phishing, security threats)
- Ensure confidentiality when using external services (e.g. GDPR and CJEU decision on US operated services)
    - Consider both the primary contractor and any subcontractors.
    - How are/were security incidents handled in the past by the contractor?

2.5.2 Mitigation:

- Segmented networks (as above 2.5)
- Backups:
    - Test reliability of backed up data
    - Test restoration
        - How long does it take, what systems are critical, does it actually work? Practice.
- Redundant fail over
    - Segregated system, authentication, and so on (Effectively a second independent system) for mission critical systems

- Using Uninterrupted Power Supply (UPS) to prevent data loss; both for servers and readers, e.g. TLD reader
- Software pre-testing before using in on your live system. Test system and logging of any updates.

2.6 Data portability

The right to Data portability **"allows individuals to obtain and reuse their personal data for their own purposes across different services".** They have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format" (see article 20 GDPR).

According to a quite recent study done by IAPP, data portability is still "an obscure data subject right" [11].

There is not yet unified legal coverage on this topic; therefore, it is usually (and partially) covered by the national transposition of the GDPR Directive (or additional Data Protection Laws).

Important aspects:

Data Portability covers personal data provided by the data subject to a controller, by their consent, or in the context of a contract that is processed in an automated manner.

What data provided by the data subject is, it is still unclear. However, there are two types:

1. "Observed" / Generated data
2. Raw data

However, we should not forget that the main purpose of Data Portability is to prevent the "vendor lock-in" phenomenon. That means that a person must be provided, while changing the data controller, the **necessary and sufficient** data in order to be automatically imported into the new system (untouched, via a delegation/import mechanism, machine to machine, ideally). The right to portability still exists for dose records, e.g. where the data subject moves between employers, or countries.

☺	If you store data in a structured manner (SQL or equivalent), you can export easily either in SQL or in XML/JSON the necessary information, with minimal development effort.
☹	Do you have the necessary mechanisms in place to be able to see the entire user "history" in your system? E.g. do national radiation protection regulations cover this area?

3 GDPR - Right to be Forgotten

European REGULATION 2016/679 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), covers the main issues concerning data protection and regulation.

Concerning "the right to be forgotten", the EU REGULATION 2016/679 establishes the following:

- "After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, **unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.**" (81)
- "The processor, at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies **unless Union or Member State law requires storage of the personal data.**" Article 28. 1 (g).

European Union "Technical recommendations for monitoring individuals for occupational intakes of radionuclides", Radiation Protection Nº 188 (2018) [12], specifies that:

- **Dosimetry records should be confidential** and should be preserved in a manner approved by the competent authority.

According to the Council Directive 2013/59/EURATOM of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom and 2003/122/Euratom:

- **The record containing the results of individual monitoring for each category A (and each category B worker if so required by the Member State) shall be retained** during the period of their working life involving exposure to ionising radiation and afterwards **until they have or would have attained the age of 75 years**, but in any case **not less than 30 years after termination of the work involving exposure.**

Therefore:

- Personal data and dose records should be confidential and should be preserved in a manner approved by the competent authority (national regulatory bodies or equivalent).
- Personal data and dose records cannot be deleted upon request and must be retained until the exposed worker reaches or would have reached 75 years of age and not less than 30 years after termination of the work involving exposure. This might not apply to IMS's for the specific country.
- Individual Monitoring Services will advise their clients/users that personal data and dose records will be retained for legal pruposes, and they may be required in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process. This provision must be accepted by the client before the provision of the service.

Possible paragraph for contract[1]:

In accordance with legal requirements of Council Directive 2013/59/EURATOM, your personal and dose data will be collected and retained during your working life involving exposure to ionizing radiation until you have, or would have, reached the age of 75 years, but in any case, not less than 30 years after termination of the work involving exposure. The use of our service implies that you agree to the collection and storage of information in relation to this policy.

We may disclose your information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements). We will not use or share your information with anyone except as described in this Privacy Policy.

At the end of this time, you have the right to have your personal data deleted. If a valid request for removal is received and no exemption applies, we will delete all your data from our backup systems as well as live systems.

[1] It's recommended that the IMS provide this information to employers to pass on to the workers.

4 GDPR Data Minimization

Dose record keeping is the making and keeping of personal dose records for radiation workers. It is an essential part of the process of monitoring the exposure of individuals to radiation and shares many of the same objectives as individual monitoring. The purpose of record keeping, the nature and scope of the records that are kept, the extent of record keeping systems and the information provided are influenced by national requirements[13,14].

According to article 5 of GDPR "Principles relating to processing of personal data" collected data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

As far as an IMS is concerned, the purpose of data collection could be described as:

"the maintaining of records of radiation doses to workers, together with the necessary associated information, to enable employers to comply with relevant radiation protection legislation."

APPLYING DATA MINIMIZATION

Data processed (collected, stored, shared with, etc.…) shall be:

- Sufficient to properly fulfil the purpose stated by the IMS ,
- Rationally linked to that purpose
- Limited to what is necessary

Data minimization process

The data minimization principle requires entities to process (collect, store, share, etc…) only 'adequate, relevant and limited' personal data. EU data protection law does not define what 'adequate, relevant and limited' means but states that the assessment of what is 'necessary' must be done in relation to the purposes of processing.

In accordance with this principle, by default, only the amount of personal data that is necessary for the processing shall be processed. "Amount" refers to quantitative as well as qualitative considerations. Moreover, both the volume of personal data, as well as the types, categories and level of detail must be taken into consideration.

The minimization procedure could be consisted of the following steps:

- **Identification of the necessary data for the purposes of processing**: The key to an efficient data minimization process is to be clear about what and why it is needed.
- **Clear definition of processing time.** This could be a major issue as, in many cases, there are other obligations, requirements or regulations demanding long periods of keeping dosimetry data.
- **Correction of inadequate data**: Keep data as current as possible (by working with individuals and customers to update their data) and cultivate optimized databases.
- **Limitation of access**: The dosimetry service must define who (organisations, radiation officers, health services etc. …) can have access to personal data based on an assessment of necessity. Furthermore, the number of persons who have privileged access to customers' personal data should be minimised.
- **Strategic deletion:** in accordance with progressive evaluation protocols, remove any unusable or incorrect information. Consistently purge stale data to ensure the information

stored is truly valuable. Consider the new data needed as well as any outdated types of information that no longer serve the purpose of processing.

- **Reduction of degree of identification**: If the purpose of the processing does not require the final set of data to refer to an identifiable individual (such as in statistics) then data should be anonymised.
- **Review the whole procedure regularly**

☺

- Narrow data collection: Collect data which is only absolutely necessary
- Avoid collection of sensitive data: a dosimetry service manages customers' doses that are sensitive data. More sensitive data, such as health data, should not be collected
- Minimize the access control: Set strict parameters to control the number of privileged accounts that have access to that data
- Periodically review: Periodically check if the data is still relevant and adequate, and delete anything no longer needed.

☹

- Too Much Data
  - Have more personal data than needed to achieve the specific purpose.
  - Data includes irrelevant details.
  - Collect particular information from all customers instead of certain individuals, when needed. The result of this action is to process information that is likely to be excessive and irrelevant.
  - Collect data on the off-chance that it might be useful in the future.
- Inadequate Data
  - Collected data is not helping to achieve the intended purpose
  - Collected data is based on an incomplete understanding of the facts and the purposes.
- Uncontrolled data storage
  - Keeping copies of documents on too many places

DATA MINIMIZATION BENEFITS

- Reduced risk of data loss, exposure to data theft and other security threats
- More efficient data retrieval and storage
- Enhanced customers' approval: People prefer to be asked for less personal data, and trust those who provide assurances about data storing
- Allows prompt responses to data subject requests

A simple check list as the following proposed by Information Commissioner's Office website could be helpful [15].

☐ We have sufficient personal data to properly fulfil our purposes.
☐ We only collect personal data we actually need for those purposes.
☐ We periodically review the data we hold and delete anything we don't need.

5 Summary of Privacy of Personal Data, GDPR & Dosimetry

The General Data Protection Regulation (GDPR) is a strict law on privacy and security and imposes obligations on organizations wherever they collect data relating to individuals in the EU. The GDPR requires organizations to protect personal data in all its forms. Moreover, GDPR changes the rules of consent and strengthens people's privacy rights.

Although the principles of the GDPR are simple, the regulation itself is complex, far-reaching and light on specifics. This makes GDPR compliance a daunting prospect, particularly for small and SMB such as a dosimetry service (IMS).

The GDPR imposes harsh fines on those who violate privacy and security standards, with fines amounting to tens of millions of euros.

The GDPR applies to the processing of personal data that is both automated and non-automated and includes information related to an individual who can be identified or is identifiable, directly or indirectly, from that information.

What is Personal Data?

Personal data is any information that is or may be related to a natural person that can be identified directly or indirectly through this information. Names and email addresses are by-default personal data, while location information, ethnicity, gender, biometric data, religious beliefs, web cookies and political opinions can also be considered as a personal data.

The following personal data is considered to be "sensitive" and is subject to specific processing conditions:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- data concerning sex life or sexual orientation

Table 2. Personal data example

Personal Data	"Sensitive" Personal Data	Not personal data
Names	Medical records	Anonymised data
Email addresses (name.surename@domain.net)	Political stance	Email addresses without personal information (info@domain.net)
Location information	Racial or ethnic origin	Information about legal entities (companies, authorities…)
Home address	Biometric data (fingerprints, pattern of the iris.)	Data related to a deceased person

☺ Are the dose records sensitive personal data? As health-related data of course they are.

☹ Pseudonymized data is still personal data? According to GDPR, yes, it is considered to be personal data if the process can be reversed

When is data processing allowed?

Article 6 lists the cases in which the processing of personal data is legal:

- The data subject has given specific, explicit consent to the processing of the data.
- Processing is necessary to execute or prepare a contract to which the data subject is a party.
- The data process complies with a legal obligation or is needed to save somebody's life.
- Processing is necessary to perform a task in the public interest or carry out some official function.
    - There is a legitimate interest in processing personal data. Although it is the most flexible part of GDPR, the "fundamental rights and freedoms of the data subject" always override processor interests, especially if it's a child's data.

☺ IMS should only have and process personal / sensitive data that is absolutely required to fulfil its contractual and legal obligations.

Data privacy and Data protection

Data protection and data privacy are, by no means, the same terms. "Data privacy" refers to proper usage, collection, retention, deletion and data storage. Data protection is policies, methods and means to keep those data safe and secure.

A Dosimetry service maintains a large amount of information related to individual monitoring persons to fulfil its obligation against its customers, organization and national authorities. According

to article 32 of GDPR, an IMS must have appropriate technical and organizational processes established to meet GDPR standards. Among others measures in this article are proposed:

- - The pseudo-anonymization and encryption of personal data;
- - The ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- - The ability to restore the availability and access to personal data promptly in the event of a physical or technical incident;
- - Regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
- - The appropriate level of security depending on the risk.

GDPR- Rights of the Data Subject

General Data Protection Regulation aims to empower individuals and give them control over their data. The GDPR outlines eight distinct rights that all Data subjects are entitled to and that an organization must uphold through data processing. Chapter 3 of the GDPR records those rights as the Rights of the Data Subject.

Table 3. The 8 Rights of Data subject and the corresponding articles in GDPR

Data Subject Rights	GDPR Article
Right to Information	Articles 13 and 14
Right of Access	Articles 15
Right to Rectification	Article 16
Right to Erasure	Article 17
Right to Restriction of Processing	Article 18
Right to Data Portability	Article 20
Right to Object	Article 21
Right to Avoid Automated Decision-Making	Article 22

Each of the user rights reflects the principles of accountability and transparency that run through this legislation.

5.1 Data protection principles

GDPR, in Article 5.1-2 outlined seven protection and accountability principles that every data processor shall take into account:

- Accountability: GDPR compliance must be proven and demonstrated.
- Accuracy. Personal data shall be accurate and up to date.
- Data minimization. Data shall be limited to what is necessary.
- Lawfulness, fairness and transparency: Processing shall be lawful, fair and transparent to the data subject.
- Purpose limitation: Data process is allowed only in case of legitimate purposes, specified explicitly to the data subject.
- Storage limitation: Personally identifying data must be stored for as long as necessary for the specified purpose.
- Integrity and confidentiality: Processing must be performed in such a way as to ensure appropriate security, integrity and confidentiality.

The principles of GDPR data privacy are quite simple. The law requires a data processor to make a good-faith effort to give people the means to control how their data is used and who has access to it.

To facilitate this, a Dosimetry service needs to provide monitored persons, with transparency and openness, all the information they need to understand how their data is collected and used.

Furthermore, a Dosimetry service needs a clear policy for the person who is the data subject to exercise the various rights.

In particular, a Dosimetry service must inform its customers, in detail, about the type of data it maintains, explaining how it has the right to process that data and for which time interval.

Finally, customers must be informed about their rights concerning their personal data and how they can exercise these rights.

Appendix 3 presents a detailed summary of GDPR and Dosimetry.

6 Conclusion

This document aims to provide dosimetry services with guidance on how to handle their data in a secure and digital manner. However, this is not always straightforward, as employees and managers of dosimetry services may not possess in-depth backgrounds in IT, data storage, and encryption. It is therefore crucial that this document be used as a guide for dosimetry services to communicate their needs to the responsible IT services within their company or institution.

Not only will IT services need to contribute, but legal services will also need to assist dosimetry services in correctly implementing GDPR legislation. Interdisciplinary collaboration will be of great importance here, as the translation of GDPR legislation into dosimetric data must then be further implemented into the practical aspect of data storage and encryption.

Communication will be key to properly implementing the needs of the services regarding their dosimetric data and correctly storing and protecting it. The need for further harmonization regarding IT services for the dosimetry leads to more guidelines on 'how to' to ensure correct implementation of legislation into the methods of the dosimetry services.

References

1. O'Reilly, J. *Network Storage: Tools and Technologies for Storing Your Company's Data*; **2016**; ISBN 9780128038659.
2. Trikha, B. A Journey From Floppy Disk to Cloud Storage. *Int. J. Comput. Sci. Eng.* **2010**.
3. Deng, Y. Deconstructing Network Attached Storage systems. *J. Netw. Comput. Appl.* **2009**, doi:10.1016/j.jnca.2009.02.006.
4. Tate, J.; Lucchese, F.; Moore, R. Introduction to Storage Area Networks. *Contract* **2006**.
5. Liu, A.; Yu, T. Overview of Cloud Storage And Architecture. *Int. J. Sci. Technol. Res.* **2018**.
6. Ju, J.; Wu, J.; Fu, J.; Lin, Z. A survey on cloud storage. *J. Comput.* **2011**, doi:10.4304/jcp.6.8.1764-1771.
7. Liu, K.; Dong, L.J. Research on cloud data storage technology and its architecture implementation. In Proceedings of the Procedia Engineering; **2012**.
8. Rajan, R.A.P. Evolution of Cloud Storage as Cloud Computing Infrastructure Service. *IOSR J. Comput. Eng.* **2012**, doi:10.9790/0661-0113845.
9. EU REGULATION 2016/679 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 Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (accessed on Mar 2, **2023**).
10. online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311 (accessed on Mar 2, **2023**).
11. No Title Available online: https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/ (accessed on Mar 2, **2023**).
12. *Technical recommendations for monitoring individuals for occupational intakes of radionuclides*; **2018**;
13. Council Directive 2013/59/EURATOM of 5 December 2013 laying down basic safety standards for protection against the dangers arising from exposure to ionising radiation, and repealing Directives 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Eurato Available online: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:013:0001:0073:EN:PDF#:~:text=This Directive establishes uniform basic,dangers arising from ionising radiation (accessed on Mar 2, **2023**).
14. Ambrosi, P., Garcia-Alves, J., Bartlett, D. *Technical recommendations for monitoring individuals occupationally exposed to external radiation*; **2010**.
15. online: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (accessed on Dec 4, **2024**);

Appendix 1

BACKUP IMPLEMENTATION, AN EXAMPLE

The following is an example that should be seen as inspiration rather than a guide for a specific implementation. Other methods will be appropriate for different IMSs, depending on their context. This example concentrates on ZFS (Zeta File System) for data integrity and backups as the ZFS file system has some unique capabilities that simplify data management. Additionally, it looks at how to add backup to a single system (dose management system in this example). Similar setup should be repeated for all the segments.

A separate NAS (Network Attached Storage), see Figure A1, for storage of data (this allows several computers/servers to access and work on same data) that has access controls limited so that only those systems/people who absolutely need access have it, and, even then, it is limited to read-only access if sufficient. The NAS is running ZFS based RAIDZ3 (any three drives can fail without data loss) with snapshotting (effectively taking an image of data as it is to allow going back in time) and scrubbing (in ZFS language this means periodically checking all the data and correcting any inconsistencies found) enabled. The combination of cheap (as in amount of storage) snapshots and ability to detect and repair corrupt data is very specific to ZFS, as it is the only mature high reliability file system available. This makes it effectively the only really good choice for data storage. It is well supported on FreeBSD and Linux, and there are distributions (like TrueNAS Core/scale) based on ZFS that makes running a NAS relatively simple.

To provide fast recovery backup, there is a second ZFS based NAS in, preferably, a remote location running as a backup unit. Access controls for the two NASs are separate and there are no shared credentials. The first NAS is synchronising each snapshot (can be as often as each minute as it only stores changed data) to the backup NAS with access control that allows it to upload snapshots but does not allow any management of snapshots already there. This ensures that even if someone has access to the primary NAS they will not be able to damage the backups.

Even so, it is good practice to have offline backups. Offline backups are immune to any kind of remote compromise and are thus the safest backup for critical data. However, this comes at the cost of a certain amount of manual labour (if the system is automated it is not truly offline).

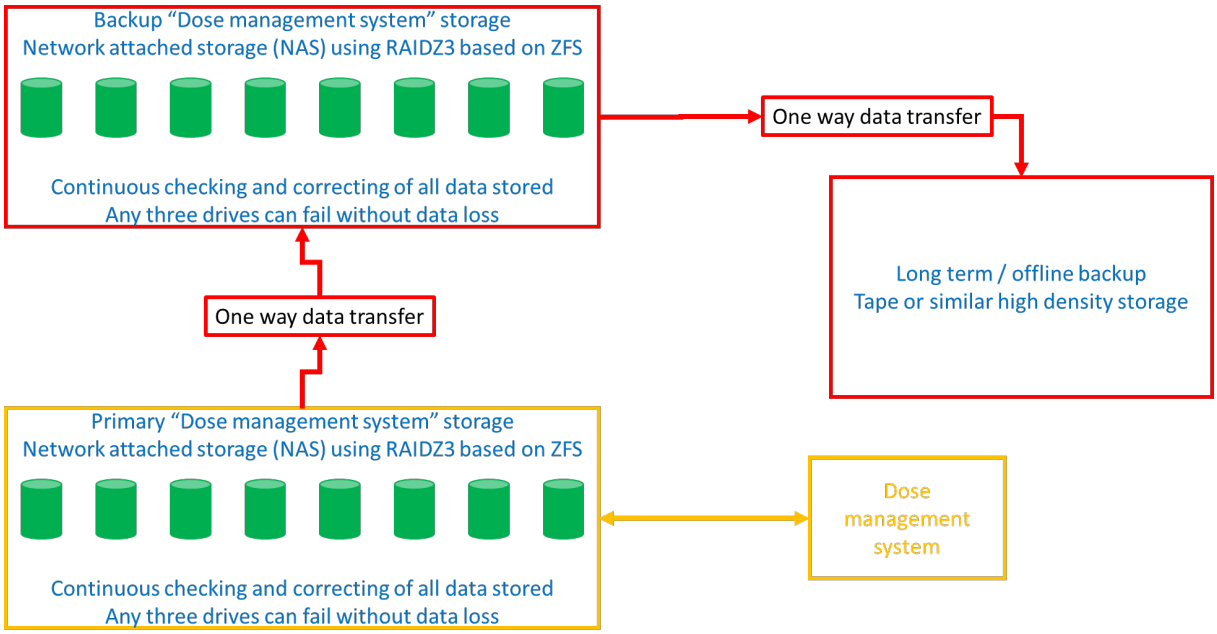

Figure A1. Example of backup setup for one of segmented networks/systems.

This basic setup can be extended with additional NASs to provide real-time failover capabilities, load balancing and other such features. That does not change the basic rules of segmentation of access control/network, integrity checking, and backups.

Appendix 2

RISK ASSESSMENT

IMS logo	**Risk Assessment**					
Date of Risk Identification						
Activity in the process	*Description of the activity, step or object being analysed*					
Identified Risk	*Description of what can go wrong / wrong*					
Potential Risk Effect	*What is the impact on the validity of the results or the quality policy*					
Severity [S]	*How serious is the impact on the customer*					
Potential causes	*What is the cause of the deviation*					
Probability of Deviation [P]	*How often this is likely to happen*					
Way of Control	*What are the existing controls that prevent deviations from occurring or being recognized in the event of an occurrence*					
Likelihood of Detection [D]	*How easy it is to detect an error*					

IMS logo	**Risk Assessment**					
RPN	*Risk Prioroty Number*					
Recommended measures / Opportunities	*What measures or opportunities can reduce the occurrence of causes or improve the detection of deviations*					
Responsibility	*Who is responsible for the recommended measures / opportunities*					
Deadline	*Recommended date / period for the implementation of the measures*					
Measures Taken	*What measures have been taken to reduce the risk*					
[S]	*Severity*					
[P]	*Probability of occurrence*					
[D]	*Likelihood of detection*					
RPN2	*Risk Prioroty Number after applied measures*					

Appendix 3

GDPR AND DOSIMETRY CHECKLIST

A. General

1. Overview:

General Data Protection Regulation (GDPR): Data protection right of individuals and improve the free flow of personal data in the digital single market.

Replacing Directive 95/46/EC harmonization in 28 Member States

2. Material scope

- GDPR applies to:
  - Processing of personal data – Dosimetry data processed electronically
  - Processing of data which form part of a filing system- Dosimetry data in hard copy filing system

- Excluded:
  - Processing of personal data by a natural person in personal activities
  - Use of data by authorities for prevention or investigation of criminal acts or for protection of public security
  - Outside of EU law

3. GDPR applies to:

- EU Companies- **EU operators of places where ionizing radiation takes place and EU dosimetry services providers**
- Non EU companies but processing personal data of subjects in the EU- **Non EU dosimetry services providers, monitoring**

B. General Principles, Legal Ground, Consent and Sensitive Data

4. General Principles:

- Lawful, fair and transparent
- For specified, explicit and legitimate purposes- purposes for dosimetry defined by law: health, security, safety at workplace, protection of citizens.
- Adequate, relevant and limited to what is necessary
- Accurate and where necessary kept up to date. Need for data retention **policy to be defined from regulatory obligations regarding dosimetry data**
- Kept no longer than necessary
- Protected in an appropriate way by technical and organizational measures- Need **a security policy covering dosimetry data**

5. **Legal ground: Obligation to found every processing on:**
- Consent of the data subject- consent of employees and can always be withdrawn
- Performance of a contract
- Controller is subject- Obligation of controller, i.e. **Operator of places where ionizing radiation takes place; regulatory obligation of operator to monitor exposure to radiation**
- Protection of vital interest of data subject
- Performance of a task carried out vested in the controller- Reliance on consent to be limited to cases where it is the only way of justifying the processing activity.
- Legitimate purposes of the controller or third party

6. **Consent: Obligation to demonstrate of the consent with specific requirements**
- Clear and plain language
- No implied consent
- Consent to all purposes
- Free choice
- No power imbalance
- Unbundled consent
- Not tied to contract
- Withdrawable
- Explicit sensitive personal data

7. **Sensitive data**
- Racial or ethnic origin
- Political opinion
- Religious of philosophical belief
- Trade union membership
- Genetic data, biometric data for identification purpose
- **Data concerning health**
- Person's sex life or sexual orientation

8. **Processing sensitive data is prohibited, except:**
- Data subject give explicit consent- employees
- Necessary for the rights and obligations of the employment and social security laws- Employment and social security regulatory obligations of controller, operator of places where ionizing radiation takes place.
- To protect vital interest
- Personal data made public by the subject
- in establishment of exercise or defense of legal claims
- Public interest-public health
- Preventive or occupational medicine
- Archiving purpose in the interest

C. Accountability

9. **Accountability: Companies will be able to demonstrate respecting the principles of the GDPR.**
- Obligation of controller- operator of places where ionizing radiation takes place
- Develop a formal data protection compliance program

10. **Awareness:**
- Obligation to take appropriate measures to reduce the risk of violation of the GDPR -approved codes of conduct or an approved certification mechanism, training to senior management to comply with obligations under the GDPR and the risks in case of non-compliance, appoint a responsible senior manager for the implementation of the data protection policy
- Demonstrate that data protection is being taken seriously- assessing taking into account the nature, scope, context, purposes of processing as well as the risks for data subjects- foresee a budget, reporting to the senior management about data protection

11. **Data protection officer (DPO). Designate a data protection office when**
- core activities of the company consist of processing operations which require regular and systematic monitoring of data subjects- operators and dosimetry services, dosimetry as regular and systematic monitoring
- Processing sensitive or criminal data- dosimetry
- Required under Member state law

12. **Records of processing activities: Obligation to maintain a record of processing activities, data record, under its responsibility:**
- Not obligatory when company has less than 250 employees, except when hold risk rights and freedoms of the data subject, is frequent, sensitive or judicial data.
- Information is different for the controller and processor- controllers and processors, record of processing activities, develop policy about data record and to keep it up date. Appoint a responsible for keeping the record

13. **Training. Obligation to ensure that DPO organizes enough training for the other employees- implementing training on GDPR, consider training or awareness raising**

14. **Data protection impact assessments (DPIA) is obligation to conduct in certain cases of high risk processing, including seeking advice from Data Protection Officer (DPO) and prior consultation with supervisory authorities.**
- Obligation for processors to provide support
- Develop policy with processes for the execution of the data protection impact assessments
- Develop a standard data protection impact assessment
- Implement the data protection impact assessment, if it is required
- Consult the supervisory authority, if it is required

15. Privacy Design and by Default. Obligation to:

- Build in data protection (privacy) in products and services
- Process data which are necessary for the processing and only make data available for an unknown number of persons by human intervention
  - Develop policy lines in order to be able to meet obligations
  - Strive for data minimization
  - Use applications and processes which meet the conditions for Privacy by Design and Privacy by Default
  -

16. Codes of Conduct and Certification

- Possibility to endorse approved codes of conduct and get itself certified; it can contribute to the demonstration of compliance with the GDPR.
  - Dosimetry could be subject of codes of conducts and certification
  - Consider participation in the development of codes of conduct and certifying mechanisms
  - Follow up of the publication of the codes of conduct

D. Right of the Data Subjects

17. Right to information (transparency). Obligation of controller to provide information to the data subject regarding the processing.

- Modalities:
  - Information includes: Contact details of the data protection officer
    Legal ground
    Legitimate interest (in cases this is a legal ground)
    Storage period
    Right to data portability
    Possibility to withdraw consent
    Right to lodge a complaint
    Data source
    Mechanism for international transfer
  - Information has to be provided in:
    - ✓ A concise, transparent, intelligible and easily accessible form
    - ✓ Using clear and plain language in writing or by other ways
    - ✓ Free charge
- To check
  - Existing privacy notices on the processing of dosimetry data on their conformity with information obligations and update privacy notices
  - Compliance of information obligation for each processing activity and every category of data subjects and develop new privacy notices
  - When timing and how form the information obligation can be met (privacy policies)

18. Right to access. Obligation of controller to give data subjects:

- Certainty about the processing of their personal data
- Information regarding the processing
- Access to their personal data
- Modalities:
  - Free or charge
  - Copy
  - Within a month (exceptionally extend by 2 months)
  - Right to request additional information about the identity of the data subject
- Be aware that data subjects may request access to dosimetry data
- Develop a standard procedure regarding the right to access, including verification of the identity of the data subject (controller)
- Develop processes and procedures to make the right to access technically possible (controller+ processor)

19. Right to erasure ("right to be forgotten"). Obligation to:

- Erase, in certain circumstances, the personal data at the request of the data subject
- In case the data were made public, take reasonable steps to inform the controllers which are processing the data of the requests by the data subject to erase his personal data
- Inform the recipients of personal data of the request of the data subject to erase its personal data
- Modalities:
  - Free or charge
  - Within a month (exceptionally extend by 2 months)
  - Right to request additional information about the identity of the data subject
- To do:
  - Develop a standard procedure regarding the right to erasure, including verification of the identity of the data subject (controller)
  - Develop processes and procedures to make the right to erasure technically possible (controller+ processor)

20. Right to restrict processing. Obligation to:

- In certain cases, and at the request of the data subject, restrict the processing of his personal data
- In case of restriction, limit the processing to storage (exceptions)
- Modalities:
  - Free or charge
  - Within a month (exceptionally extend by 2 months)
  - Right to request additional information about the identity of the data subject
- To do:
  - Develop a standard procedure regarding the right to restrict the processing, including verification of the identity of the data subject (controller)
  - Develop processes and procedures to make the right to restrict the processing technically possible (controller+ processor)

21. Right to data portability. Obligation to:

- In certain cases, follow the request of the data subject, to obtain his personal data and to reuse them as he wishes
- Transfer data directly to another controller (when technically possible)
- Modalities:
  - Free or charge
  - Within a month (exceptionally extend by 2 months)
  - Right to request additional information about the identity of the data subject
- To do:
  - Relevance limited for dosimetry data, as the right to data portability ONLY applies to data processed (by automated means) on basis of consent of data subject or contract with the data subject, while dosimetry data are most often processed on basis of legal/regulatory obligation.

22. Automated decision-making, including profiling

- Obligation to ensure for some automated decisions: Data subjects obtain human intervention, give their point of view, are given an explanation for the automated decision, and that they can challenge that decision
- Only for decisions which produce legal effects or similarly significantly affects data subject and relevance for dosimetry data limited.

E. Security

23. Security obligation to:

- Implement appropriate technical and organizational measures to protect the personal data
- Take measures in order to ensure that those acting under authority only process data by order of the controller
- Inform supervisory authorities within 72 hours with regard to data breaches
- Inform data subjects without undue delay about data breaches which are likely resulting in a higher risk
- Keep a record of data breaches (including consequences and measures taken)

- Modalities which are necessary proceed to
  - Pseudo-anonymization or encryption
  - Guaranteeing the confidentiality, integrity, availability and robustness of the IT systems
  - Developing procedures to restore in time availability of and access to personal data in case of a physical or technical accident
  - Periodical evaluation of mechanisms used to guarantee security of personal data Processor has to inform the controller about each data breach without undue delay
  - Notification to the data subjects is not required when data is unintelligible/encrypted, export measures were taken so that the high risk for data subjects is avoided or when notification would take disproportionate efforts

- To do:
  - Check current security measures in the light of the GDPR (controller + processor)
  - Consider appointing another responsible person with whom all breaches can be notifies and who will subsequently follow up (controller)
  - Implement procedures to ensure deadlines can be met (controller + processor)
  - Analyse which processing activities imply a high risk to the data subjects (controller)
  - Implement procedures which make it possible to, where necessary, immediately inform data subjects and also take the necessary measures (controller)
  - Make a record holding data breaches and measures taken (controller)

F. Transfer to third countries

24. No transfers to countries outside of EU, except (in case of one of the following conditions are met):

- Data is being transferred to a country, a territory or sector which ensures an adequate level of protection
- Transfer is subject to appropriate safeguards: binding corporate rules (BCR), standard data protection clauses (SCC), codes of conduct, or certification
- Transfer is subject to one of the following exceptions: explicit consent of the data subject, transfer for the performance of an agreement, transfer necessary for the vital interests of the data subject who cannot express his consent
- Transfer is necessary in the public interest
- Transfer is necessary in the light of the execution of a legal claim
- Transfer from a public register
- Limited transfer
- To do:
  - Analyse the transfers to third countries and map them
  - Check legal grounds and whether these are still lawful under the GDPR
  - Implement adequate guarantees (standard contracts, binding corporate rules, etc.) if necessary
  - Check consent clauses
  - Check agreements regarding data transfers, including subcontractors (back-to-back)

G. Processors

25. Processor has the obligation to:

- Appoint a representative when established outside of the EU
- Include certain minimum clauses in contracts with controllers
- Obtain consent of the controller when outsourcing the processing, additionally certain minimum clauses need to be included in the outsourcing contract
- Process data according to the instructions of the controller, unless Union or Member State law requires otherwise
- Keep a record of the processing on the account of the controller
- Collaborate with the supervisory authorities
- Take appropriate technical and organizational security measures

- Inform the controller of any breach with regard to personal data
- Appoint a data protection officer in certain circumstances
- Comply with rules on the transfer to third countries
- To do:
  - Amend/update existing service contracts between operators and dosimetry service providers in light of requirements GDPR
  - Amend /update template service agreements (dosimetry service providers)
  - Be aware of direct obligations under GDPR and additional contractual obligations (dosimetry service providers)

H. Sanctions

- Supervisory authorities will be able to issue fines of up to 4% of annual worldwide turnover or €20 million, whichever is greater.
- Supervisory authorities will have the power to audit, issue warnings and issue a temporary and permanent ban on processing
- Individuals can sue for compensation to recover both material and non-material damage
- To do
  - Review your current level of compliance and bring it up to the level required under GDPR
  - Consider overall attitude to risk and consider creating a risk assessment framework