

EUROPEAN  
BLOOD  
ALLIANCE

## Data Protection in the Blood Sector: Challenges for Blood Establishment Data Protection

Author: Sabrina Keenan, Chair EBA DPO/Privacy Officers Working Group

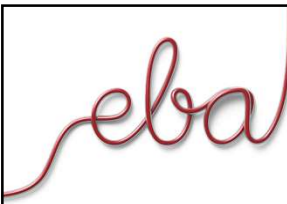
February 2021



EUROPEAN  
BLOOD  
ALLIANCE

### EBA DPO/Privacy working group

- EBA DPO/Privacy working group set up early 2018
- Discussion re challenges of implementing the new GDPR regulation in the blood establishment context
- Aims and objectives - information sharing, research, providing guidance, opinions, position papers



EUROPEAN  
BLOOD  
ALLIANCE

## GDPR Principles

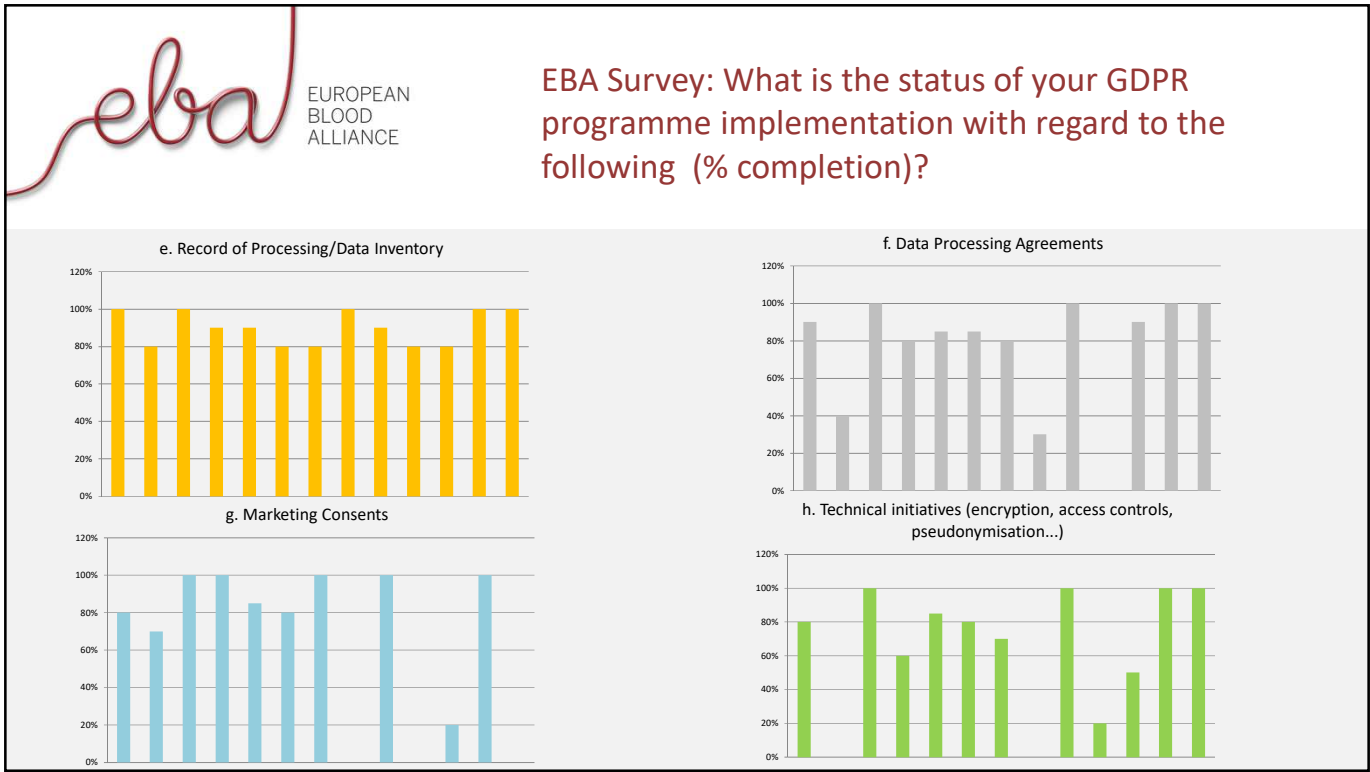
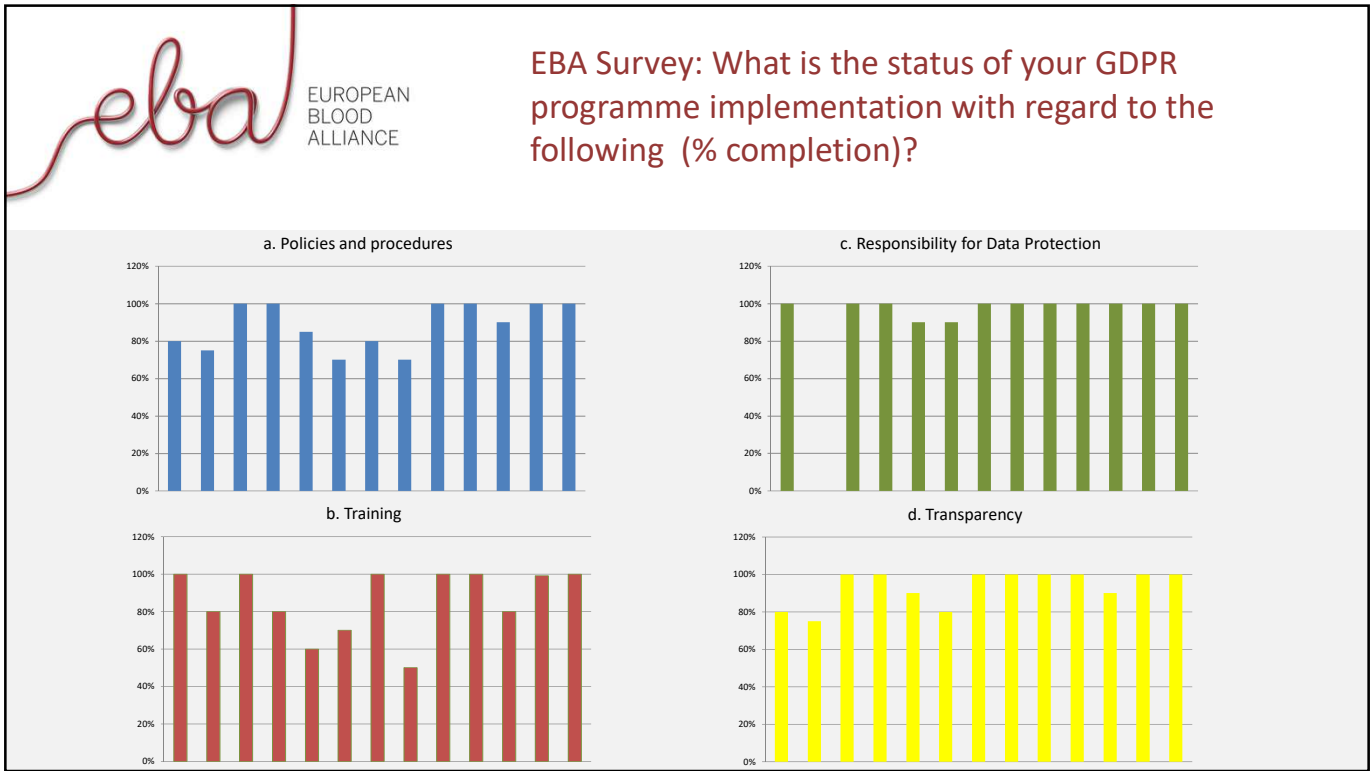
1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimisation
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability



EUROPEAN  
BLOOD  
ALLIANCE

## Meeting the Principles of GDPR – EBA Survey on GDPR Implementation Feb 2020

- Ireland, UK, Greece, Germany, Croatia, Serbia, Portugal, Finland, Malta, Belgium, Luxembourg
- Survey Areas
  - Responsibility for Data Protection
  - Policy and Procedure
  - Training
  - Transparency and Data Subject Rights, Consent
  - Mandatory Records of Processing
  - Data Protection Agreements
  - Technical Requirements
  - Complaints, Breach and Regulatory





- eba EUROPEAN BLOOD ALLIANCE
- ### Question: Challenges your organisation has experienced during your GDPR implementation?
- On-going awareness
  - Resourcing
  - Managing multiple parties
  - Interface of GDPR with other legislation
  - Data Controller and Data Processor responsibilities
  - Differing interpretations of GDPR
  - SAR's
  - Software/System limitations
  - Unclear/lack of guidance
  - Data protection by design and default
  - Internal collaboration
  - Data sharing
  - Research
  - Data minimisation
  - Lawful basis for collecting sensitive data
  - Interface with regulator
  - Internal circulation of information
  - Marketing

## Question: Opportunities which have arisen during your organisations GDPR implementation?

- Data minimisation requirement supports destruction of archive data
- Clarification of business processes
- Conscious and responsible handling of data
- Raised awareness of data protection issues and raised profile of info security and info governance
- Opportunity to design data protection into processes from the start

## Some final specific considerations

1. Right to be Forgotten
2. IT Systems - bespoke, audit trail v right of erasure, limitations for archive, encryption, pseudonymisation, privacy by design and default
3. Laboratory Instruments – generating more data
4. Data sharing – with hospitals, other government bodies and the need for agreements and/or legislation
5. Culture and Mindset – collecting ‘all of the data’ for medical or QA investigations v collecting the right data
6. Conducting Research – transparency requirements, data protection in ethics applications