

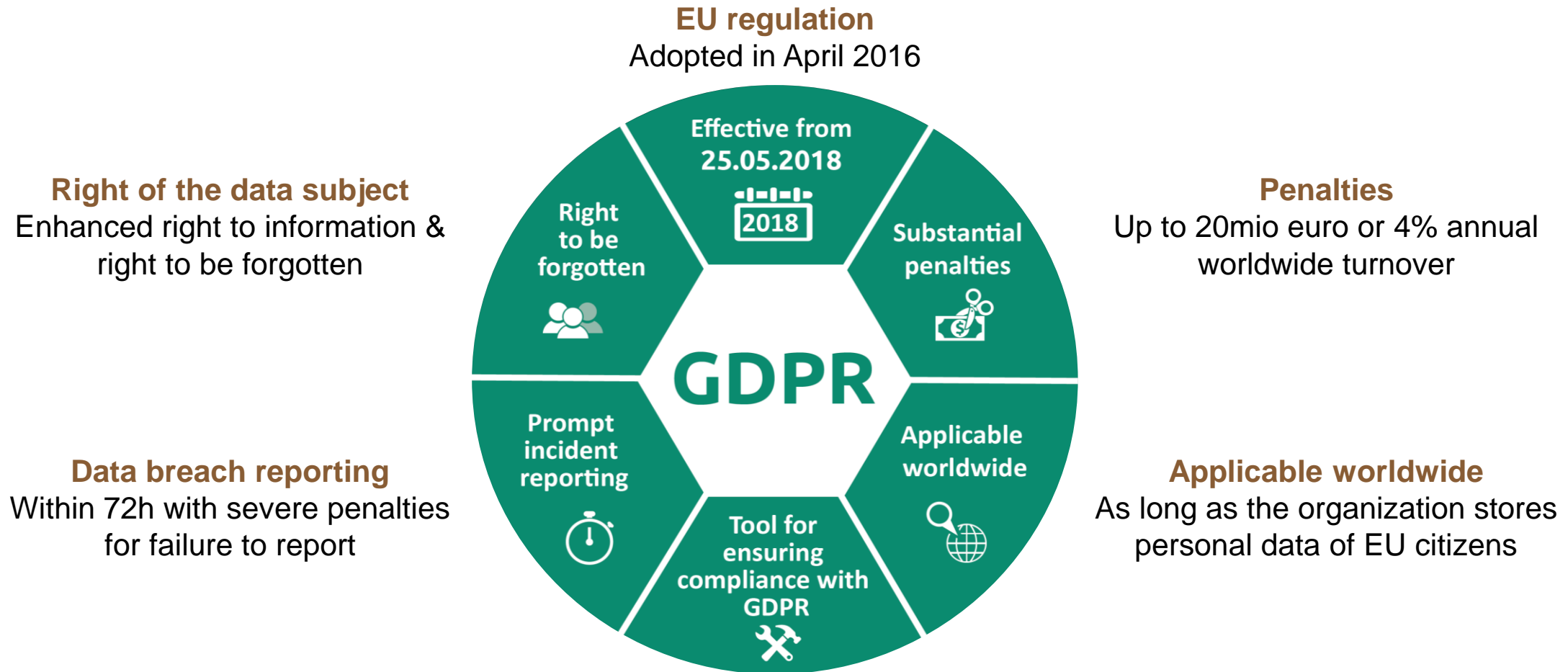


GLOBAL DATA PROTECTION REGULATION (GDPR) – FIBA 2018 PROJECT

GAIFS WORKSHOP – LAUSANNE MAY 28TH 2018



WHAT IS GDPR ?



Sources

<https://www.eugdpr.org/eugdpr.org.html>
<http://gdprcoalition.ie/>
<http://www.trustarc.com/blog/tag/gdpr-privacy/>
<https://www.dlapiper.com/en/uk/focus/eu-data-protection-regulation/key-changes/>

LARGE VOLUME & VARIETY OF DATA

FIBA Employees

FIBA HR manages recruitment for all legal entities of the FIBA group (incl. regional offices)



Transfers (incl. minors)

FIBA requests various personal data during transfer proceedings, especially in case of minors



Accreditation

FIBA keeps data of accreditation holders



3x3 Platform

Worldwide online register of players. Passport scans required for top players



Eligibility

Documents containing sensitive and/or personal data (e.g. passports) are requested.



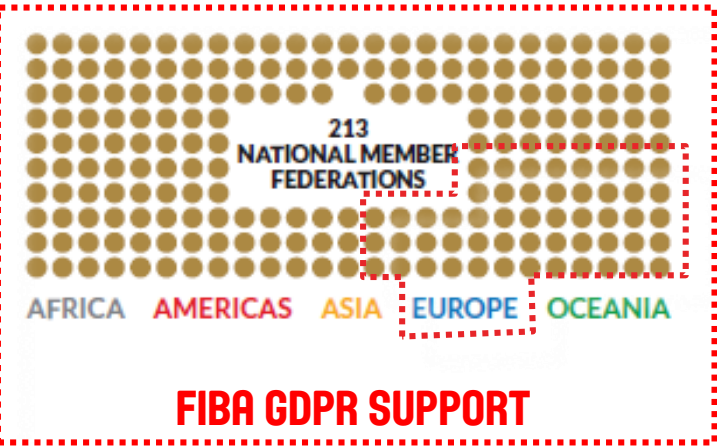
Disciplinary / Anti-Doping

Documents containing sensitive and/or personal data are requested and processed in disciplinary proceedings.

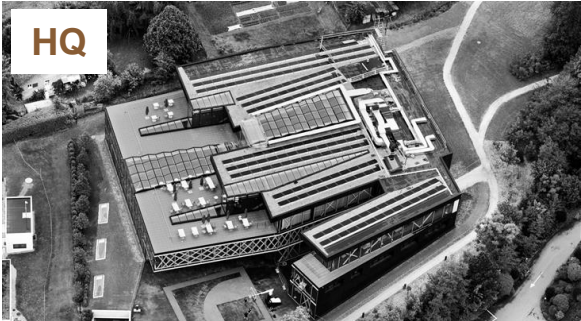


FIBA IS A COMBINATION OF BODIES AND PARTNERS MANAGING DATA ACROSS THE WORLD

Data on Players (eg. transfers) & competitions



FIBA GDPR COMPLIANCE PROJECT



Players, Competitions, Fans, Employees

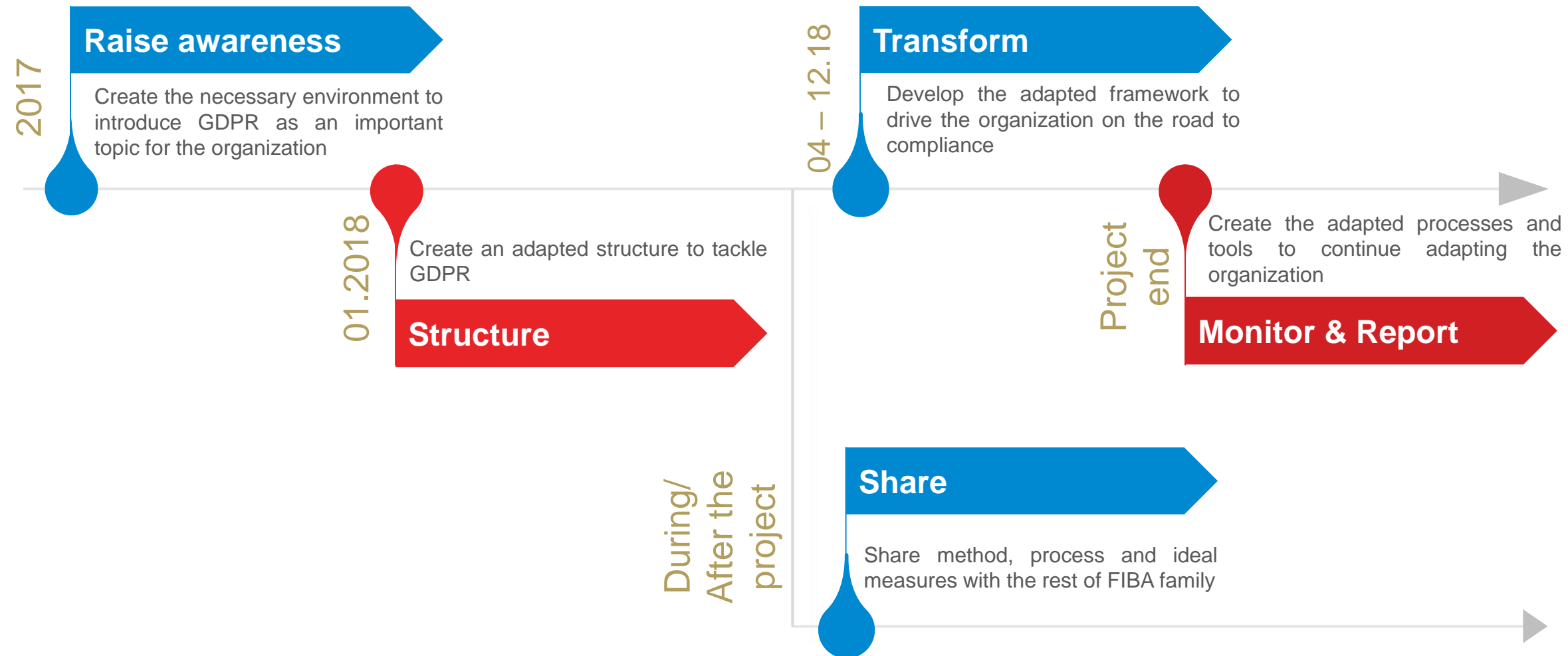
Regional Office AFRICA	Regional Office AMERICAS	Regional Office ASIA	Regional Office EUROPE	Regional Office OCEANIA
<ul style="list-style-type: none"> • Competitions • National Federations & Sport • Administration 	<ul style="list-style-type: none"> • Competitions • National Federations & Sport • Administration 	<ul style="list-style-type: none"> • Competitions • National Federations & Sport • Administration 	<ul style="list-style-type: none"> • Events • Competitions • National Federations & Sport • Administration 	<ul style="list-style-type: none"> • Competitions • National Federations & Sport

Regional offices

Data on players, competitions
Data for communication and marketing use



FIBA ADOPTED A REALISTIC TIMELINE FOR ITS GOAL TO COMPLIANCE



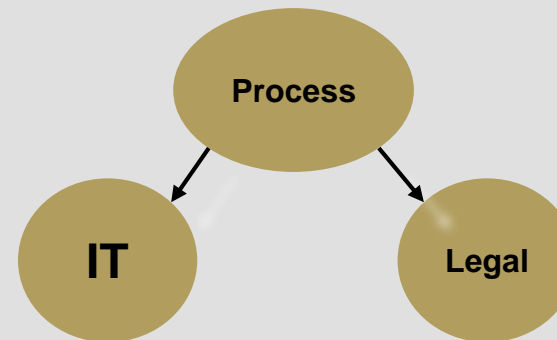
FIBA ADOPTED A FRAMEWORK IN 6 STEPS TO ALIGN STRUCTURE & PROCESSES

Key challenges

- Tackle GDPR by the right angle
- Define what you really need for your organization

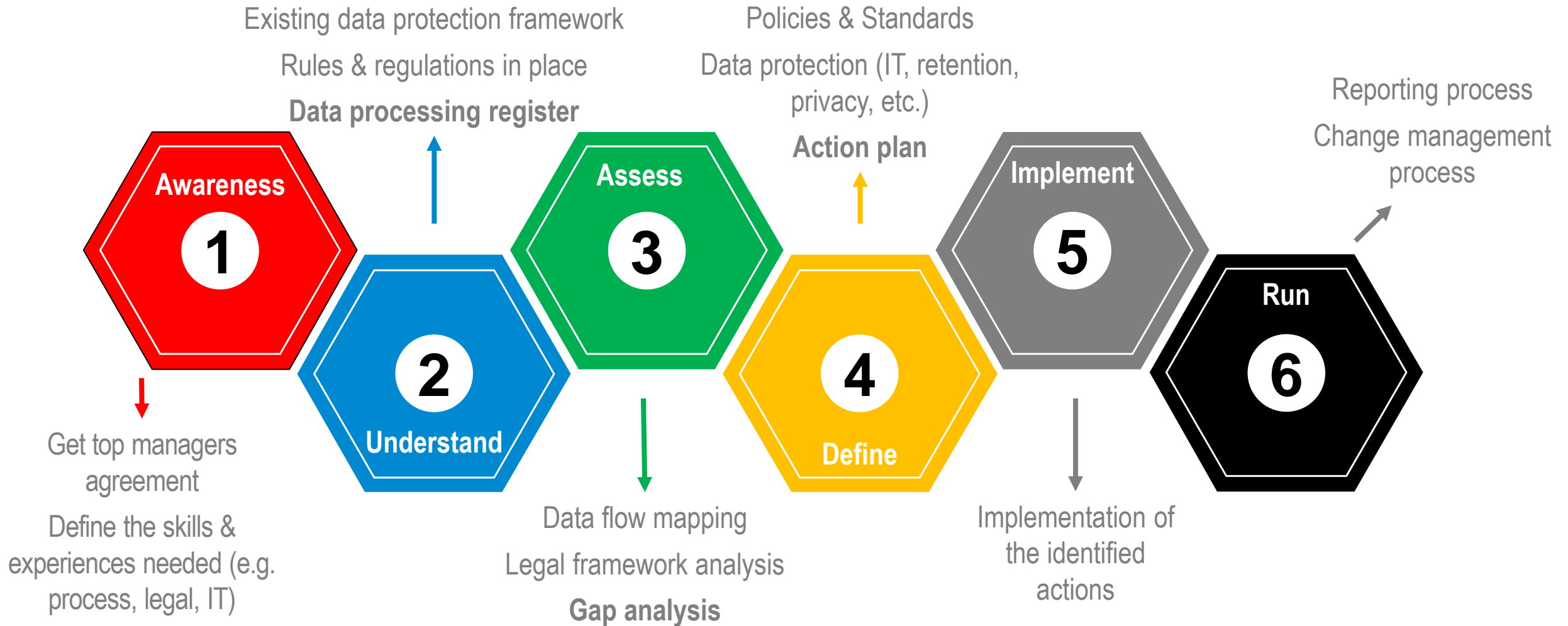


What is the right angle to look at it ?



FIBA looked at it with a general approach (not technical, neither legal)

FIBA ADOPTED A FRAMEWORK IN 6 STEPS TO ALIGN STRUCTURE & PROCESSES



INVENTORY OF PROCESSING ACTIVITIES



Objectives

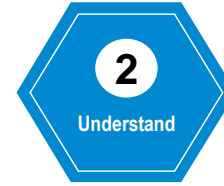
- Creating an overview of how personal data is processed within the organization and develop the register of personal data processing activities.

Deliverables

- Register of personal data processing activities

Controller contact details					
Company name					
Address					
Description of the processing					
Name of the processing					
Purpose of the processing					
Legal grounds for processing					
Categories of affected individuals					
Categories of personal data		Description		Time limit for erasure	
Applications supporting the processing		Description		Type of recipient	
Security measures					
Technical security measures					
Organisational security measures					
Categories of recipients		Description		Type of recipient	
Cross-borders transfers		Recipient	Country	Safeguards	Link to docs
Recipient organisation 1					
Recipient organisation 2					

Source : PriceWaterhouseCoopers



INVENTORY OF PROCESSING ACTIVITIES

Activities

- HR – Recruitment, personal files and payment of salaries, etc.
- Media & Marketing – Marketing campaigns, web analytics, etc.
- Communication – Newsletter for fan engagement, advertising, general promotion, etc.
- IT – Workstation monitoring, IT services, etc.
- Legal affairs – Anti-doping, contracts, recording of legal proceedings, etc.
- Facility management – Video surveillance, accesses, etc.
- Travel management – Travelers information, accommodation bookings, etc.
- Sports & Competition – Players, referees, volunteers, athletes transfer, etc.
- CSR – Management of social and humanitarian initiatives, etc.
- Disciplinary – Management of disciplinary cases, etc.

GAP ANALYSIS



Objectives

- Review organization's data protection capabilities, provide an overview of the existing compliance level and identify gaps with the EU-GDPR, based on 8 specific domains and criteria.

Deliverables

- Summary of key data protection capabilities
- Summary of key constraints, describing areas of improvement
- Overview of identified gaps with the EU-GDPR.
- A list of recommendations to improve the capabilities and achieve compliance.

GAP ANALYSIS



Domain	Criteria description
1. Strategy, Governance and Accountability	Designated resources coordinate and maintain responsibility for the data protection programme (e.g., defining programme objectives, establishing across functional governance structure, demonstrating compliance, overseeing and implementing training).
2. Individuals' Rights and Processing	A method is established to determine justifications for the data processing and to manage lawful grounds, such as consent or legitimate interest. Special attention is paid to the grounds for processing special categories of data. Individuals' rights (to rectification, to be forgotten, to object, to restrict, of access) and associated requests are managed effectively.
3. Data Protection Notice and Policy Management	Data protection policies, notices, procedures and guidelines are formally documented and are aligned and consistent with applicable laws and regulations. Data protection policies are reviewed and approved. Additionally, data protection notices are accessible in clear and plain language.
4. Risk Management and Compliance	A data protection risk management programme is documented, approved and adopted in order periodically to identify and mitigate material risks that could result in the unauthorised collection, use or disclosure of regulated data. A process is defined to evaluate and monitor the effectiveness of the data protection programme.
5. Data Lifecycle Management	A process is established to inventory and classify data to help identify areas of risk and set expectations for required safeguards. Additionally, a process is established to maintain data accuracy and comply with record retention requirements. Data protection is embedded in FIBA's practices and systems, including in cases of cross-border transfers.
6. Incident Response and Breach Management	Policies and procedures are established to triage suspected breaches of information and ensure timely and thorough incident management. The process specifies how FIBA will respond to a confirmed breach of data, including notifications of appropriate parties. The plan is subject to testing at planned intervals or upon significant changes.
7. Third Party Risk Management	Data protection requirements for mitigating the risks associated with third party access to information assets are agreed and documented prior to granting access to such third parties. Third parties and their access to and use of FIBA's information and systems are regularly monitored, reviewed and audited for compliance with contractual security and data protection requirements.
8. Data Security	Personal data is protected to ensure the continuing confidentiality, integrity and availability of information.

Source : PriceWaterhouseCoopers

ACTION PLAN

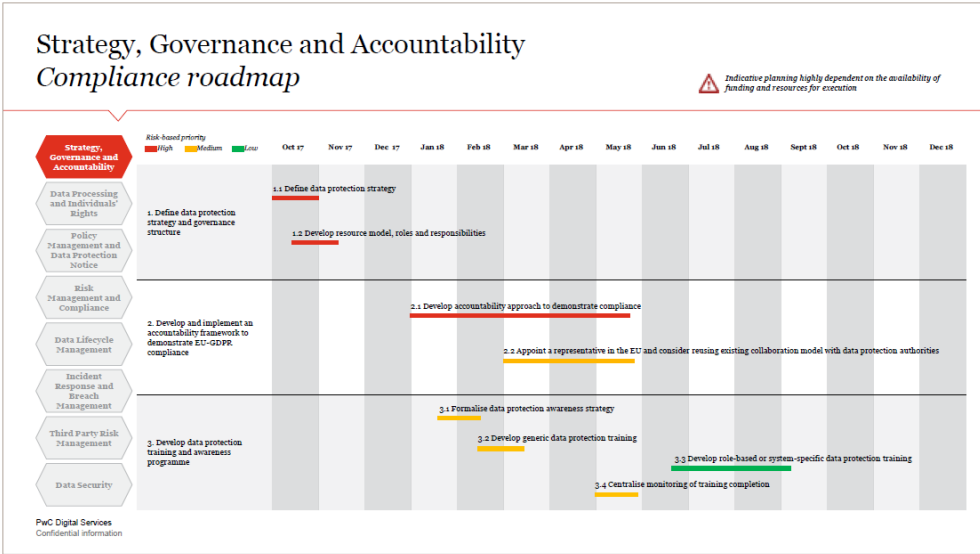


Objectives

- Develop the compliance roadmap to address identified gaps, including the following steps :
 - A global privacy strategy and structure
 - Improved policies and procedures
 - A privacy risk management strategy
 - A data life cycle management
 - A enhanced existing data governance structure

Deliverables

- Detailed risk-based implementation specifications and guidelines
- A forward looking program



FIBA WILL IMPLEMENT A SIMPLE OPERATIONAL PROCESS TO MONITOR CHANGES AFTER THE PROJECT



Evaluate changes : resources,
impacts, complexity, etc.

Train champions to identify data
management changes related to the
regulation and policies in place



Validate changes evaluation and
implementation at a high governance
level

Implement a change management
process (reporting process) for data
protection and data management
changes

Identify data protection owners in the
different business units to raise
awareness for any changes in the
future



SEBASTIEN MIAZZA
PMO & RISK SENIOR MANAGER

+41 22 545 00 00

SEBASTIEN.MIAZZA@FIBA.COM

