**WHAT IS GDPR?**

**EU regulation**
Adopted in April 2016

- **Right of the data subject**
  - Enhanced right to information & right to be forgotten

- **Data breach reporting**
  - Within 72h with severe penalties for failure to report

- **Penalties**
  - Up to 20mio euro or 4% annual worldwide turnover

- **Applicable worldwide**
  - As long as the organization stores personal data of EU citizens

Sources
https://www.eugdpr.org/eugdpr.org.html
http://gdprcoalition.ie/
http://www.trustarc.com/blog/tag/gdpr-privacy/
LARGE VOLUME & VARIETY OF DATA

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

Accreditation
FIBA keeps data of accreditation holders.

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

Transfers (incl. minors)
FIBA requests various personal data during transfer proceedings, especially in case of minors.

3x3 Platform
Worldwide online register of players. Passport scans required for top players.

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.

FIBA GDPR Compliance Project

Data on Players (eg. transfers) & competitions

Data on players, competitions, Fans, Employees

Data for communication and marketing use

Regional offices

FIBA GDPR Support

213 National Member Federations

AFCRA AMERICAS ASIA EUROPE OCEANIA
FIBA ADOPTED A REALISTIC TIMELINE FOR ITS GOAL TO COMPLIANCE

**Raise awareness**
- Create the necessary environment to introduce GDPR as an important topic for the organization
- 2017

**Structure**
- Create an adapted structure to tackle GDPR
- 01.2018

**Transform**
- Develop the adapted framework to drive the organization on the road to compliance
- 04 – 12.18

**Monitor & Report**
- Create the adapted processes and tools to continue adapting the organization
- Project end

**Share**
- Share method, process and ideal measures with the rest of FIBA family
- During/After the project
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.

1. Awareness
   - Existing data protection framework
   - Rules & regulations in place
   - Data processing register

2. Understand
   - Get top managers agreement
   - Define the skills & experiences needed (e.g. process, legal, IT)

3. Assess
   - Data flow mapping
   - Legal framework analysis
   - Gap analysis

4. Define
   - Policies & Standards
   - Data protection (IT, retention, privacy, etc.)
   - Action plan

5. Implement
   - Implementation of the identified actions

6. Run
   - Reporting process
   - Change management process

Designed by PresentationGO.com
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

<table>
<thead>
<tr>
<th>Categories of personal data</th>
<th>Description</th>
<th>Time limit for erasure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applications supporting the processing</th>
<th>Description</th>
<th>Type of recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security measures</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Technical security measures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational security measures</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Categories of recipients</th>
<th>Description</th>
<th>Type of recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cross-border transfers</th>
<th>Description</th>
<th>Country</th>
<th>Safeguards</th>
<th>Link to data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
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

<table>
<thead>
<tr>
<th>Domain</th>
<th>Criteria Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Strategy, Governance and Accountability</td>
<td>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).</td>
</tr>
<tr>
<td>2. Individuals’ Rights and Processing</td>
<td>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.</td>
</tr>
<tr>
<td>3. Data Protection Notice and Policy Management</td>
<td>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.</td>
</tr>
<tr>
<td>4. Risk Management and Compliance</td>
<td>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.</td>
</tr>
<tr>
<td>5. Data Lifecycle Management</td>
<td>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.</td>
</tr>
<tr>
<td>6. Incident Response and Breach Management</td>
<td>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.</td>
</tr>
<tr>
<td>7. Third Party Risk Management</td>
<td>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.</td>
</tr>
<tr>
<td>8. Data Security</td>
<td>Personal data is protected to ensure the continuing confidentiality, integrity and availability of information.</td>
</tr>
</tbody>
</table>

Source: PriceWaterhouseCoopers
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

- **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.
- **Monitor** changes evaluation and implementation at a high governance level.
- **Report** changes evaluation and implementation at a high governance level.
- **Evaluate** changes: resources, impacts, complexity, etc.
- **Identify** data protection owners in the different business units to raise awareness for any changes in the future.
- **Train** champions to identify data management changes related to the regulation and policies in place.

**MONITORING & REPORTING**