Kellerhals Carrard

Data protection law – a new challenge for International Sports Federations

GDPR and what International Sports Federations must know

Bangkok, 20 April 2018

François Carrard, Dr. iur., Attorney-at-law

www.kellerhals-carrard.ch

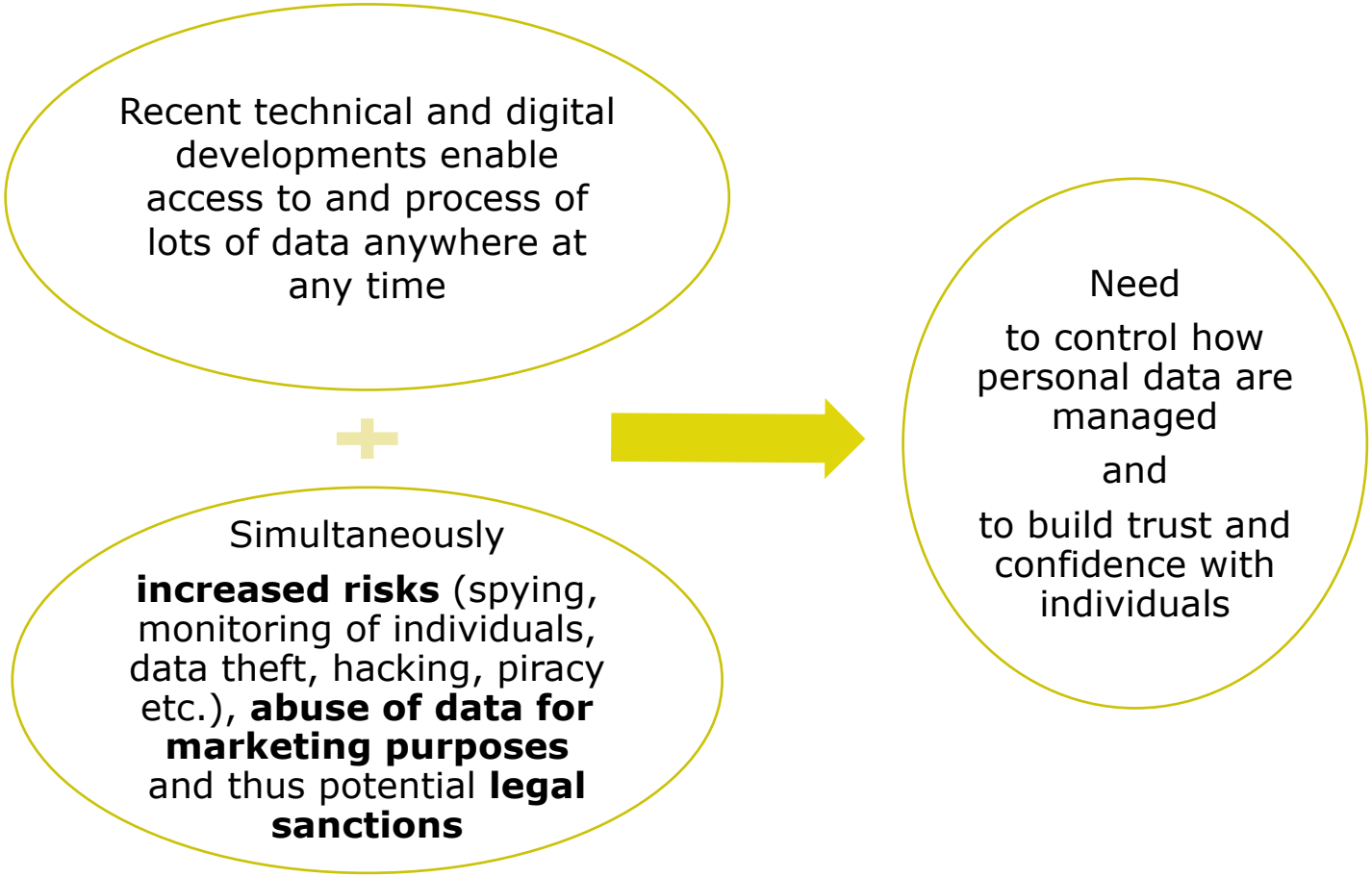
Kellerhals Carrard

AGENDA

1. **Data protection: new risks and higher responsibility**
2. **Data protection: an issue relevant for International Sports Federations (IFs)**
3. **General Data Protection Regulation (GDPR): what is it?**
4. **Other legislations**
5. **Action plan: our recommendations**

Kellerhals Carrard

1. DATA PROTECTION: NEW RISKS AND HIGHER RESPONSIBILITY



Kellerhals Carrard

Purpose of data protection rules

Depending on jurisdictions, the purpose of data protection rules is to **protect** and **empower data privacy** of:

- **individuals** and **legal persons**

  e.g. current Swiss data protection Act (to be amended)

- **individuals only**

  ⇨ e.g. new European GDPR

2. DATA PROTECTION: A RELEVANT ISSUE FOR INTERNATIONAL SPORTS FEDERATIONS (IFS)

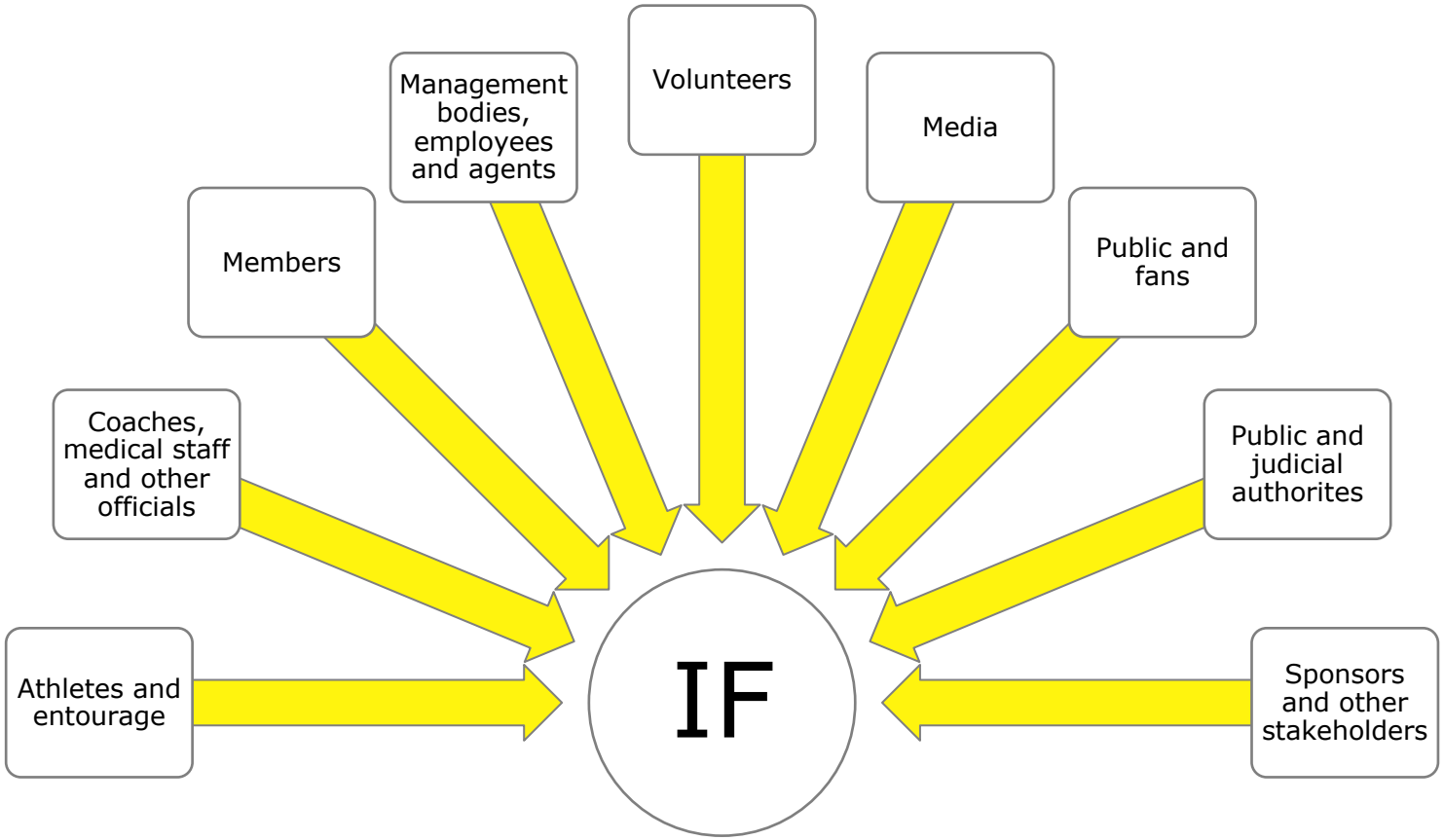
- IFs regularly **process** data, including **collect**, **transfer** and **store** personal data

- **What kind of data?**
  Personal data referring to an identified or identifiable person such as:
  - any private or professional address, including email address
  - phone number
  - social security number
  - health data and anti-doping records
  - performance data of an athlete
  - employment application form
  - bank data, credit card data

  ≠ anonymous data, provided no link can be established between the anonymous data and the person concerned

Kellerhals Carrard

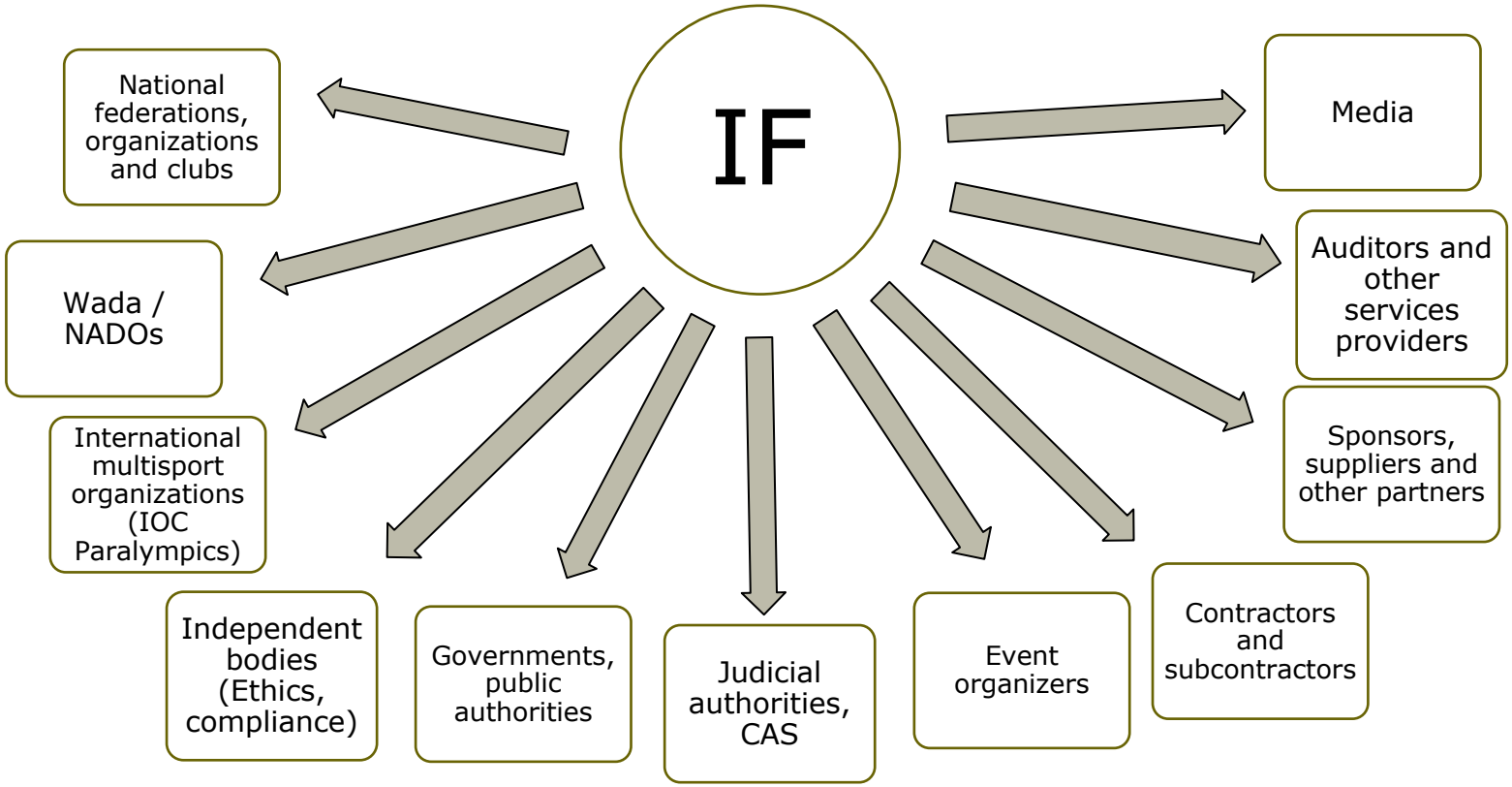
Data transmission to IF *



*** Not exhaustive**

Kellerhals Carrard

Data transmission from IF *



*** Not exhaustive**

Kellerhals Carrard

Data transmission: the athlete's path
(clubs, schools, universities, etc.)

02 – Competition registration and operations

e.g. performance data

04 – Athlete's status and contracts

e.g. sponsor, endorsement, engagement/employment

01 –License (where applicable)

03 – Anti-doping testing

e.g. sensitive health data (incl. biological passport)

Kellerhals Carrard

3. GENERAL DATA PROTECTION REGULATION (GDPR): WHAT IS IT?

What is GDPR?	• The new European regulation for the protection of personal data directly applicable in EU member states
What is the purpose of GDPR?	• Strengthening and harmonizing data protection rights for individual across EU: one single set of rules for the whole EU
What GDPR is not?	• GDPR does not aim at maintaining data security in general, such as protection business and/or manufacturing secrecy
25 May 2018	• Entry into effect of GDPR (General Data Protection Regulation)

Kellerhals Carrard

How GDPR will affect IFs

- **Extraterritorial effect of GDPR**

  GDPR will apply to any IF (inside but also outside EU) when such IF processes personal data from EU residents

  - Any activity towards individuals in EU is sufficient for GDPR to apply to IF outside EU.

- **Cross-border transfers of personal data outside EU are restricted by GDPR**

  - Adequate legal protection or additional guarantees are required when IFs transfer data outside EU.

Kellerhals Carrard

Recent event – Mark Zuckerberg's Congressional testimony

- April 4, 2018: Zuckerberg said to **Reuters** that Facebook will extend GDPR protections worldwide "in spirit" but will not apply GDPR worldwide.

- April 11, 2018: Zuckerberg said to the **US Congress** that the changes Facebook is making in response to the GDPR will be available worldwide.
  - same privacy control
  - same kinds of disclosure and affirmative consent
  - same way of treating data's user

- However no timeline on when Facebook would meet GDPR standards worldwide

Kellerhals Carrard

Changes introduced by GDPR *

- compulsory **records** of processing activities (type of data processed, why, how long, purpose, legal basis)
- extended **information** to be given to data subjects (purpose and legal basis, period of retention)
- new **consent** rules (consent by clear affirmative consent)
- **parental permission** to data processing with respect to children (< 16 years)
- new **rights** for individuals (right to access, right to erasure, data portability)
- designation of a **representative** in EU when not established in EU but engaged in certain high-risk activities
- appointment of a **data protection officer** («DPO») when engaged in certain high-risk activities
- compulsory **notification** of data breach (within 72 hours)

*** Not exhaustive**

Kellerhals Carrard

Risks in case of non compliance

- **Penalties**: fines of up to EUR 20 million or, for organizations engaged in economic activity, 4% of global annual turnover (e.g. media rights)

- **Civil litigation**: any person who has suffered «material or non-material damage» as a result of a violation has the right to receive compensation.

- **Criminal sanctions**: depending on each domestic legislation

Kellerhals Carrard

Competent authorities

- **Penalties**: data protection authorities of each Member State where individuals affected by an infringement of the GDPR reside.

  In case of transnational treatments affecting several Member States, data protection authorities will impose a joint penalty.

- **Civil litigation**: courts of the Member State where the IF has its establishment.

  Unclear when IF is not in the UE. Courts where the individuals who has suffered a damage as result of an infringement of the GDPR will likely consider themselves to have jurisdiction.

- **Criminal sanctions**: depending on domestic legislation, any criminal authorities of each Member State:
  - where individuals affected by an infringement of the GDPR reside;
  - where the IF has its establishment.

4. OTHER LEGISLATIONS

- **USA**
  - No single comprehensive national data protection law: several specific or medium-national privacy or data security laws and many laws among the states
  - No specific national data protection authority but *Federal Trade Commission* (FTC), which has authority to prevent unfair and deceptive trade practices take enforcement actions against inadequate data security measures, and inadequately disclosed information collection, use and disclosure practices

- **Russia**
  - *Federal Law No. 149-FZ on Information, Information Technologies and Data Protection 2006* and *Federal Law No. 152-FZ on Personal Data 2006* (notable amendments adopted in July 2014)
  - *Federal Service for Supervision of Communication, Information, Technologies and Mass Media* (*Roskomnadzor*)

- **China**
  - *Cybersecurity Law* (into effect since June 2017): mere broad principles
  - *Information security technology—Personal information security specification*: national voluntary standards on personal information protection to come into effect on May 1, 2018
  - No specific national data protection authority

- **Japan**
  - *Act on the Protection of Personal Information* (new amendments into force since May 2017)
  - *Personal Information Protection Commission*

- **UK**
  - *GDPR* will apply in the UK from May 25, 2018 until Brexit (March 29, 2019)
  - After Brexit: *Data Protection Bill* (not yet adopted): rules to be harmonized with GDPR
  - *Data Protection Commissioner*

Kellerhals Carrard

5. ACTION PLAN: OUR RECOMMENDATIONS

Data audit/inventory	Implementation & process	Data security measures	Record processing activities
• identification of data streams • identification of sensitive data • retention time of data • purpose of processing data • transfer of data (where/to whom)	• external and internal process • privacy policy • consent form (membership and data capture form, pop-up notice for online communication) • appropriate process in the event of data breach	• staff training • IT measures (encryption, fire walls, passwords, regular back-up) • consider appointing a DPO if engaged in high-risk activities	• build up and gather documentation • determine appropriate retention period

Kellerhals Carrard

François Carrard

Dr. iur., Attorney-at-law

Place Saint-François 1
P.O. Box 7191
1002 Lausanne

francois.carrard@kellerhals-carrard.ch