Kellerhals Carrard

General Data Protection Regulation (GDPR)

Preparing legal documentations

GAISF Workshop
Lausanne, June 19, 2018

Virginie A. Rodieux, Attorney-at-law, LL.M. | Senior Associate

www.kellerhals-carrard.ch

Kellerhals Carrard

AGENDA

1. **Importance of personal data protection**
2. **What is GDPR ?**
3. **How sports associations are affected ?**
4. **Legal basis to process personal data**
   - Recall of legal basis
   - Consent rules and re-permission campaign
5. **Enhanced rights for data subjects**
   - Recall of rights
   - Exercise of the rights
6. **New requirements**
   - Records of processing activities
   - Representative in the EU and DPO
   - Data breach
   - Processor
7. **Data flow mapping and update privacy policy**
8. **Conclusion**

Kellerhals Carrard

IMPORTANCE OF DATA PROTECTION

- Personal data are accessed and processed exponentially due to technical and digital developments
- Increased risks: spying, monitoring of individuals, data theft, hacking, piracy
- Abuse of data for marketing purposes

Need to control how personal data are managed

- to protect and empower data privacy
- to build trust and confidence

WHAT IS GDPR?

What is GDPR?	• General Data Protection Regulation: 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

Kellerhals Carrard

WHAT IS GDPR?

Some definitions

- **"Personal data"**: any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

  Even if public, personal data remain personal data.

  GDPR ≠ applicable to
  - data related to legal persons
  - data related to deceased person
  - anonymous data, provided no link can be established between the anonymous data and the person concerned

Kellerhals Carrard

WHAT IS GDPR?

Some definitions

- "**Sensitive data**"(special categories of data) : racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, sex life, sexual orientation.

- **"Data processing"**: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- **"Data subject"**: any natural person, identified or identifiable (≠ legal person)

Kellerhals Carrard

WHAT IS GDPR?

Personal data processing activities – practical cases

1. virginie.rodieux@kellerhals-carrard.ch: personal data?
2. gaisf@gaisf.org: personal data?
3. Anti-doping record of a specific athlete?
4. Paper-based client file?
5. Video of a competition where an athlete is recognizable?
6. Storing the name of attendees to a seminar after the seminar took place?

Kellerhals Carrard

EXTRATERRITORIAL EFFECT OF GDPR

GDPR applies to

1. processing of personal data in the context of the activities of an establishment in the EU
2. processing of personal data who are in the EU even though the controller or processor is no in the EU, where the processing activities of activities are related to
   - the offering of goods and services to data subject in the EU
   - the monitoring of the behaviour of data subject in the EU

Kellerhals Carrard

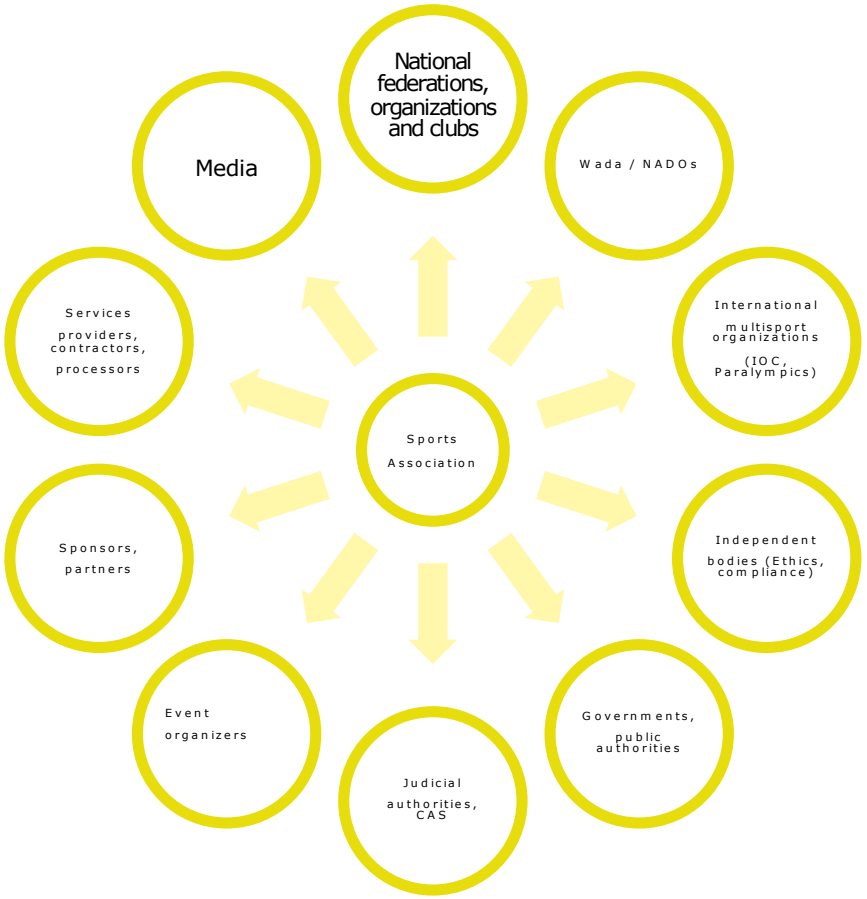
HOW SPORTS ASSOCIATIONS ARE AFFECTED?

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

- **What kind of personal data?**
  - 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

HOW SPORTS ASSOCIATIONS ARE AFFECTED?

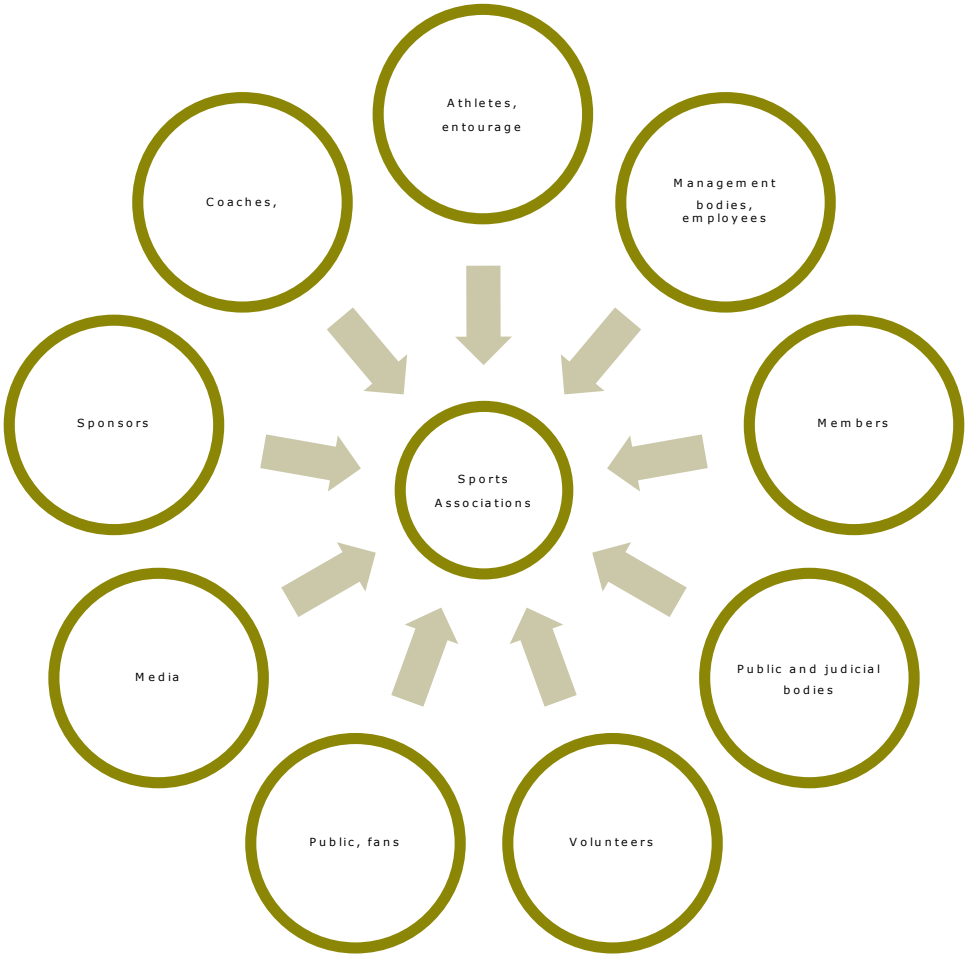
DATA FLOW FROM INTERNATIONAL SPORTS ASSOCIATIONS *



*** Not exhaustive**

HOW SPORTS ASSOCIATIONS ARE AFFECTED

DATA FLOW TO INTERNATIONAL SPORTS ASSOCIATIONS *



*** Not exhaustive**

Kellerhals Carrard

INFORMATION AND CONSENT RULES

Do

- ❑ Check consent is the most appropriate legal basis
- ❑ Ensure consent is **freely** given and confirms **specific**, **informed** and **unambiguous** agreement of the data subject to the processing
- ❑ Name your organisation
- ❑ Ask people to give consent by **affirmative** and **active** acts (e.g. written statement, ticking a box when visiting Internet)
- ❑ Request separate consent for distinct processing activities
- ❑ Inform data subject of his/her right to withdraw consent at any time
- ❑ Collect parental consent for children under 16
- ❑ Keep record of consent (how and when consent given, what data subject were told at that time)

Don't

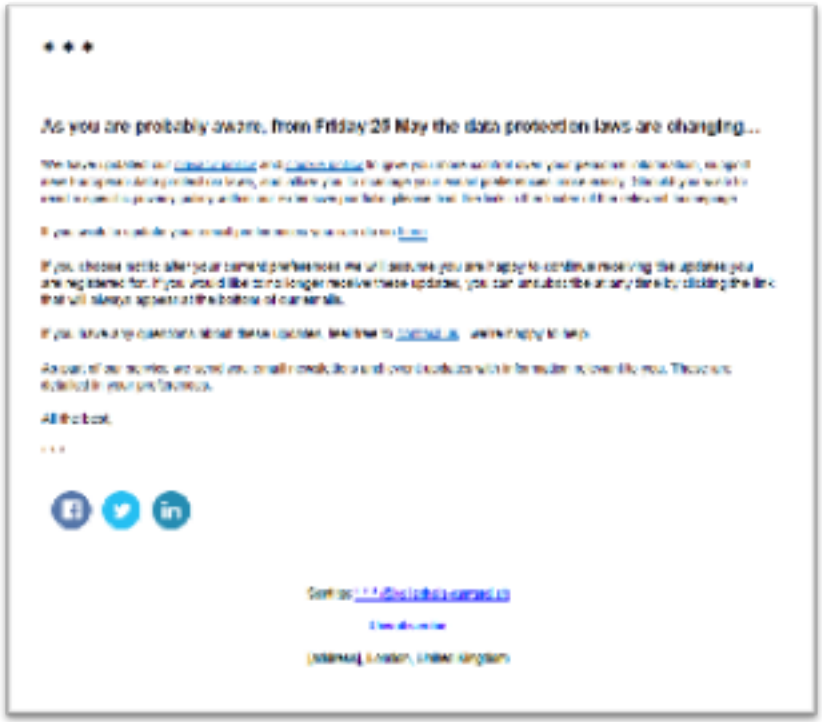
- ❑ Drown consent in other written agreements or declarations but ensure the request for consent is in a distinguishable form
- ❑ Rely on consent given by silence, inactivity or pre-ticked box
- ❑ Make consent a precondition of the provision of services

RE-PERMISSION CAMPAIGN

Opting-in

RE-PERMISSION CAMPAIGN

Opting-out



As you are probably aware, from Friday 25 May the data protection laws are changing...

We'd like to stay in touch...

Kellerhals Carrard

RE-PERMISSION CAMPAIGN

Dear * * * ,

"Nooo, not another GDPR e-mail!"

Well we're sorry to say it is... We know you have certainly received several e-mails like this one about the new General Data Protection Regulation (GDPR) that comes into effect TODAY. But we want to make sure that we are taking the necessary steps to protect your privacy and only send you communication that you are interested in!

From time to time, we will send emails to keep you informed on what's going on at * * *, as well as important news on new functionalities, product developments and invitations to our workshops, trainings and events.

We would need you to CLICK HERE to consult our privacy statement and give your consent.

So what happens if you don't click on the link above?

We won't delete you from our database but we will sadly not send you any newsletters anymore. However, if you are a client, we will keep sending you our product releases and event invitations, unless you don't want to. This preference can be changed at any time.

We sincerely hope you will take a few minutes to click on the link above so we can stay in touch ;)

Best regards,
* * * team

* * *
[address]
1007 Lausanne - Switzerland

[phone number]
[email]
[Website]

Kellerhals Carrard

RE-PERMISSION CAMPAIGN

GDPR does not require you to send re-permission email in all circumstances.

- No need of consent for data processing activities necessary for the **performance of a contract**
- No need of consent if the data processing is necessary for the purpose of legitimate interest pursued by the controller where there is a **relationship between the data subject and the controller** (direct marketing to clients may be regarded as carried out for a legitimate interest of the controller)
- No need to ask for consent if you are able to demonstrate that the data subject has consented to the data processing in line with the conditions of the GDPR

In any case, newsletters must offer the option to object against the data processing for marketing purposes.

Kellerhals Carrard

RE-PERMISSION CAMPAIGN

To do:

1. Check whether the legal basis of all or part of your data processing activities is the consent.
2. Check whether consent has already been given in the past by the data subject.
3. Check whether such past consent complies with present GDPR requirements.
4. Check whether you have proof of such past consent.

Kellerhals Carrard

RE-PERMISSION CAMPAIGN

Practical cases

1. Your regularly process data regarding your employees (name, address, social security number, etc.). Re-permission campaign needed?
2. You store data regarding volunteers who will take part in an event your are organizing in a couple of weeks (name, address, email address, etc.). Re-permission campaign needed? What about sending them newsletters after the event?

Kellerhals Carrard

ENHANCED RIGHTS FOR DATA SUBJECTS

Right of access

Right to know if data concerning him/her are treated and to obtain the communication of such data in an understandable format

Right to rectification

Right to obtain rectification of any inaccurate personal data

Right to restriction of processing

Right to restrict data processing on the following grounds:

- The accuracy of the personal data is contested by the data subject
- The data processing is unlawful and the data subject opposes the erasure
- Data non longer needed but required by the data subject for establishment of, exercise or defence of legal claims
- The data subject has objected to processing pending the verification of the legitimate grounds of the controller

Kellerhals Carrard

ENHANCED RIGHTS FOR DATA SUBJECTS

Right to erasure

Right to obtain the erasure of his/her personal data in the following circumstances:

- Data is no longer necessary for the purpose for which it was collected
- Consent on which data are processed is withdrawn and there is no other legal ground for the processing
- Data subject objects to the data processing and there are no overriding legitimate grounds for the processing
- Data have been unlawfully processed
- Deletion of data is required for compliance with legal obligation

Right to portability

Right to receive data in a structured, commonly used and machine-readable format and to transmit the data to another entity where data automated processing is based on consent or contract

Kellerhals Carrard

ENHANCED RIGHTS FOR DATA SUBJECTS

Right to object

Right to object to the processing of his/her data:

- On grounds related to his/per personal situation when processing is based on public interest task or legitimate interest of the controller unless controller can demonstrate its or a third party overriding legitimate interest
- At any time with no grounds when personal data are processed for direct marketing purposes

Kellerhals Carrard

ENHANCED RIGHTS OF THE DATA SUBJECT

How will the data subject exercise his/her rights?

- An individual may request access, in person or through a representative, by mail, email, phone or on the spot.
- In any event, before answering to such request the **identity** of the individual making the request must be verified. In case of reasonable doubt about the identity, additional information necessary to confirm the identity of the data subject must be requested (e.g. copy of passport, copy of ID).
- In case of intervention of a representative, in addition to the confirmation of the identity of the data subject, a **power-of-attorney** signed by the data subject in favour of the representative must be requested.
- Please make sure you take due note and keep record of the **date of receipt** of the access request.

Kellerhals Carrard

ENHANCED RIGHTS OF THE DATA SUBJECT

Response time

- Without undue delay and in any event within **one month** following receipt of the request
- Possibility to extend by **two months** in case of complexity and number of requests. In such a case data subject must be informed of the extension within one month of receipt of the request, together with the reason of the delay.

Form of the response

- In **writing** or, where appropriate, by **email**
- **Orally**, provided the identity of the data subject is proven
- In any event, proof of the response given must be kept. Writing or electronic form is therefore recommended.

Kellerhals Carrard

ENHANCED RIGHTS OF THE DATA SUBJECT

Any communication or actions taken in case a data subject exercises his/her right are provided **free of charge.**

Exception: reasonable fee based on administrative costs may be charged in the following circumstances:

- the request is manifestly unfounded or excessive, in particular because of its repetitive character;
- further copies are requested by the data subject.

ACCESS RIGHT – TEMPLATE OF STANDARD ANSWER

Kellerhals Carrard

ENHANCED RIGHTS OF THE DATA SUBJECT

Practical cases

1. You receive a call from Mr Legal pretending to be the attorney-at-law in charge of the defence of the interests of the athlete Mr Sport. He requests you to send him copy of Mr Sport's data you are processing.

2. A data subject requests access to his file by email on July 15, 2018. Due to vacation, the employee in charge of dealing with such emails only read the access request upon his return on August 10, 2018.

Kellerhals Carrard

NEW REQUIREMENTS

Records of processing activities

- Mandatory for the controller and the processor to keep a record of the processing activities carried out under his responsibility.
- Not mandatory for enterprises or organizations with less than 250 employees, unless the processing they perform may entail a **risk to the rights and freedoms** of the persons concerned, if it is **not occasional** or if it contains so-called **sensitive data or data relating to criminal convictions**.

  A processing is not occasional if it implies a regular treatment of the data related to the management of the personnel, the customers, etc. Most processing are not occasional.
- The record must be in writing (paper or electronic format).

  It is recommended to establish a sheet for every processing containing the above details. Every sheet must be updated and adapted according to the development of the processing. Every amendment to the processing must be reported in the sheet. There is however no need to keep in the record every single search, edit, etc.

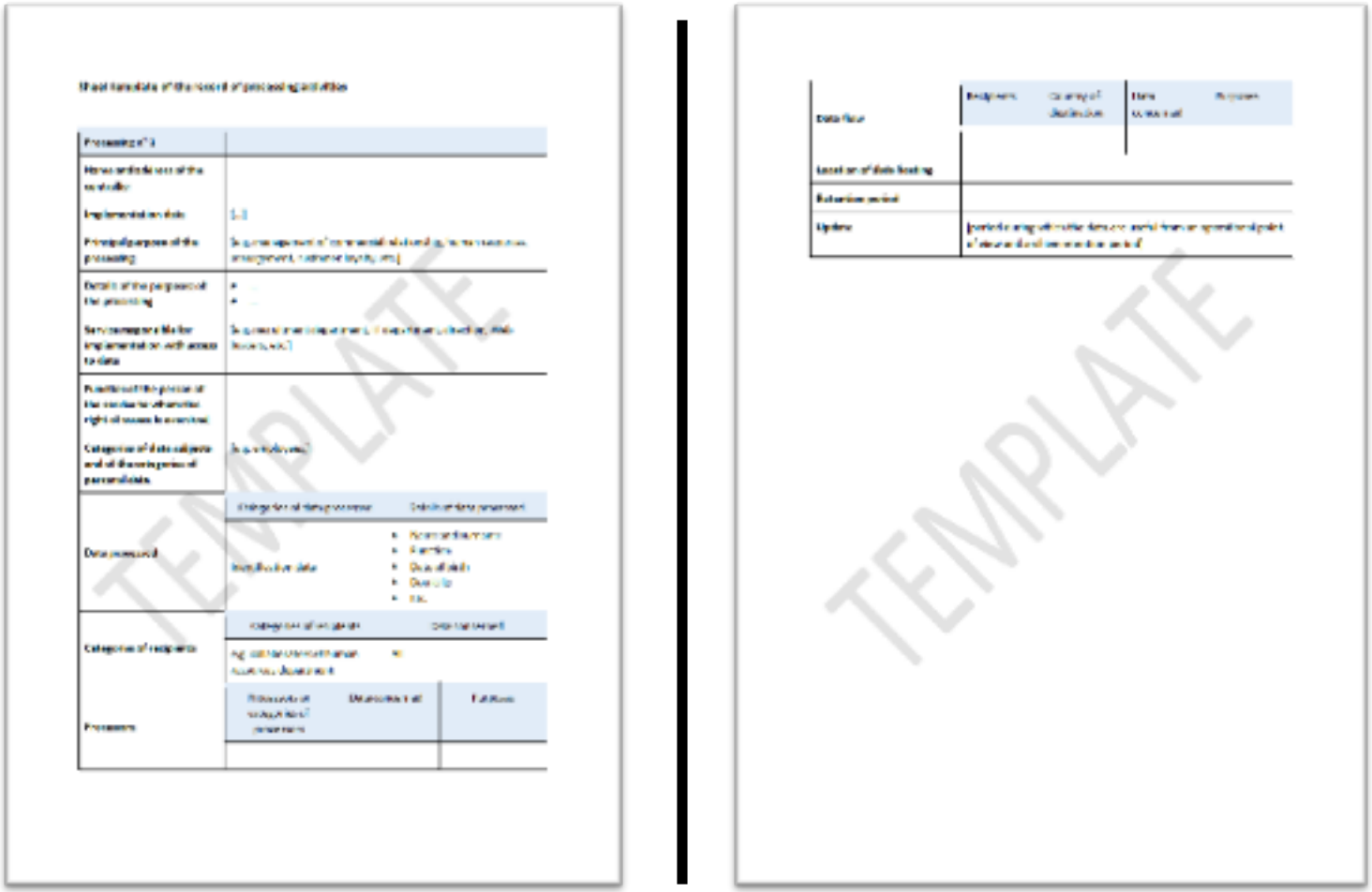
Kellerhals Carrard

NEW REQUIREMENTS

Record must contain the following information:

- the name and contact details of the controller:
- the purposes of the processing;
- a description of the categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries;
- where applicable, transfers of personal data to a third country, including the identification of that third country;
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organisational security measures.

RECORD – TEMPLATE OF STANDARD SHEET



NEW REQUIREMENTS

Representative in EU

- Mandatory for every controller or processor established outside the EU but subject to the GDPR when engaged in certain high-risk activities
- Optional for:
  - public authorities/bodies
  - when the processing is occasional, does not include, on a large scale, the processing of sensitive data or processing of data relating to criminal convictions and is not likely to generate a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purpose of the processing
- Most processing activities are permanent and not occasional.
- The representative will be the point of contact between the controller and the supervisory authorities or the data subjects for all questions relating to the processing of personal data.

Kellerhals Carrard

NEW REQUIREMENTS

Data protection officer ("DPO")

- DPO's tasks: inform and advise the controller on data protection issues, monitor compliance with the GDPR, be the point of contact for authorities and employees
- Mandatory when engaged in certain high-risk activities : carry out a regular and systematic monitoring of large-scale people or treat on a large scale so-called "sensitive" data or data related to criminal convictions or offenses

  "Large scale"? no specific indication
- Internal or external DPO but independent and no conflict of interest
- If you choose to designate a DPO where it is optional, you need to comply with GDPR requirements.
- Provide DPO necessary resources

NEW REQUIREMENTS

Data protection officer ("DPO")

To do:

1. Check whether a DPO is required and, if not, keep record of the reason of the decision.
2. Check if the appointed DPO does not have any conflict of interest.
3. If no DPO is appointed, designate a person in charge of the data protection issue. Do not call it "DPO".

NEW REQUIREMENTS

Data breach notification

Data breach: accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.

- Compulsory notification of data breach to the **authority** within **72 hours**
  Exception: breach is unlikely to result in a risk to the rights and freedoms of natural person
- Compulsory notification to the **data subject** within **undue delay**
  Exception: breach is unlikely to result in a risk to the rights and freedoms of natural person and specific measures are taken by the controller

To do: set up appropriate process in the event of data breach.

Kellerhals Carrard

NEW REQUIREMENTS

Data breach notification – practical cases *

1. Lost of a USB key where personal data encrypted are stored?
2. Cyberattack to a medical records in a hospital?
3. Cyberattack to an online marketplace – publication online of usernames, passwords and purchase history?

* Source: Group 29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250rev.01)

Kellerhals Carrard

DATA BREACH – TEMPLATE OF STANDARD NOTIFICATION


We are taking the following steps:

- We are acting immediately to notify members and to provide them with information on how they can protect their data;
- We are recommending member that they should change their account passwords;
- As a precaution, we have taken the sites offline and suspended access to the database, pending the ongoing review;
- We are continuing to enhance and reinforce our systems to detect and prevent unauthorised access to user information.

We remain at your disposal for further information. Please contact [name, function, contact details].

Yours sincerely,

[Your name]

This template is provided as an example only and needs in any case to be adapted to the specific circumstances of the case. It does not dispense you from a comprehensive analysis of the circumstances of the case, where appropriate with the assistance of a legal counsel.

Kellerhals Carrard

NEW REQUIREMENTS

Processor

- Controller must only appoint processors providing sufficient guarantees to comply with GDPR requirements.
- Parties must execute a contract or other legal act.
- Processor must only act on documented instructions from controller.
- GDPR sets out what needs to be implemented in the contract.
- Example of subcontracting contract available on the Website of the CNIL (French data protection authority): https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil_en.pdf

Kellerhals Carrard

NEW REQUIREMENTS

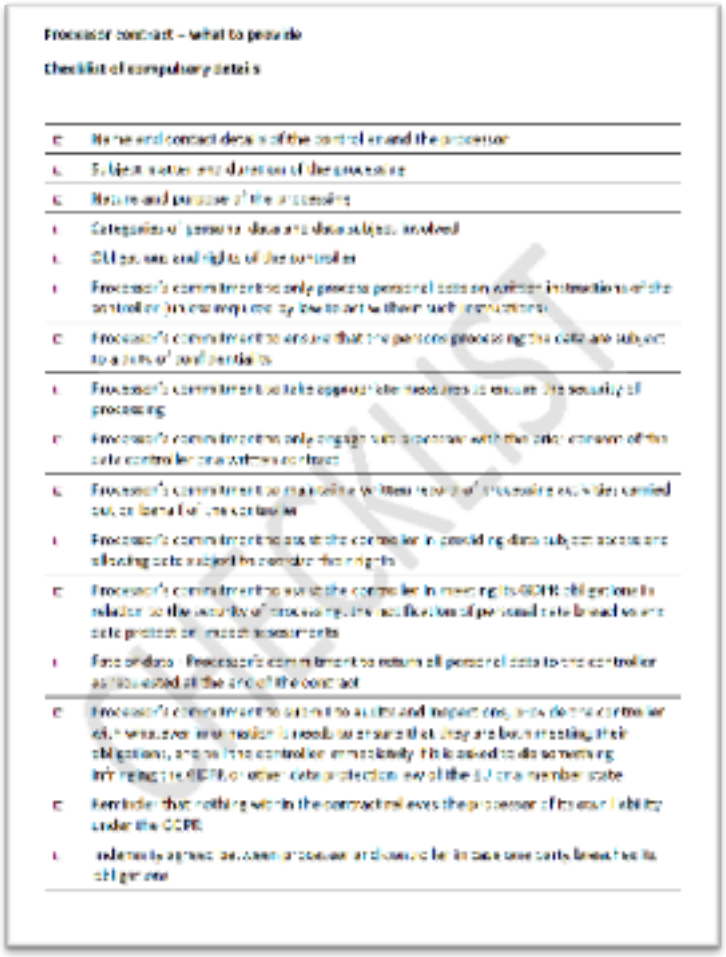
Processor

To do:

1. Check and assess any present and future agreement from GDPR point of view.
2. Make sure sufficient guarantees are provided by processors.
3. Make regular audits of processors and ask for information.

Kellerhals Carrard

PROCESSOR CONTRACT - CHECKLIST



Processor contract – what to provide

checklist of compulsory details

c	Name and contact details of the controller and the processor
c	Subject matter and duration of the processing
c	Nature and purpose of the processing
c	Categories of personal data and data subjects involved
c	Obligations and rights of the controller
c	Processor's commitment to only process personal data on written instructions of the controller (unless required by law to act without such instructions)
c	Processor's commitment to ensure that the persons processing the data are subject to a form of confidentiality
c	Processor's commitment to take appropriate measures to ensure the security of processing
c	Processor's commitment to only engage sub-processor with the prior consent of the data controller and a written contract
c	Processor's commitment to assist the controller by appropriate written technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights
c	Processor's commitment to assist the controller in ensuring compliance with the obligations relating to the security of processing, the notification of personal data breach and data protection impact assessments
c	Processor's commitment to return all personal data to the controller as requested at the end of the contract
c	Processor's commitment to submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state
c	Nonetheless, nothing within the contract relieves the processor of its own liability under the GDPR
c	Indemnity agreed between processor and controller in case one party breaches its obligations

Kellerhals Carrard

DATA FLOW MAPPING AND UPDATE PRIVACY POLICY

Data audit/inventory

- identification of data streams
- identification of sensitive data
- retention time of data
- purpose of processing data
- transfer of data (where/to whom)

Implementation & process

- 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

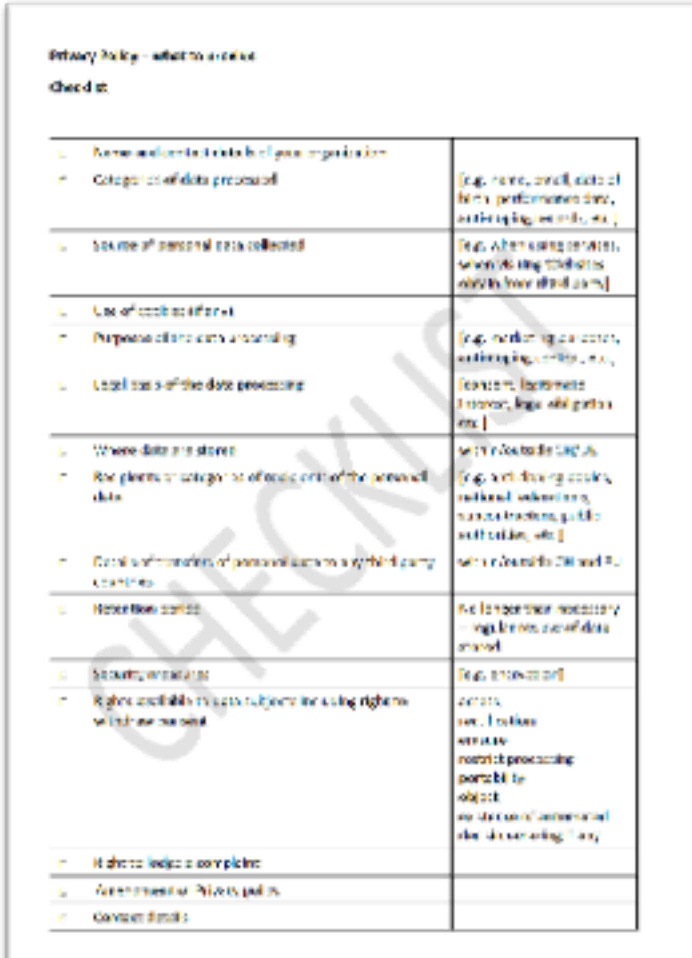
Data security measures

- staff training
- IT measures (encryption, fire walls, passwords, regular back-up)
- consider appointing a DPO if engaged in high-risk activities

Record processing activities

- build up and gather documentation
- keep a record of activity
- determine appropriate retention period

PRIVACY POLICY - CHECKLIST



Kellerhals Carrard

CONCLUSION

- Preparing and drafting legal documents is one step towards GDPR compliance: necessary but not sufficient.
- Internal process and organisation and technical measures would have to be introduced to ensure compliance with GDPR and commitments taken in privacy policy, processor subcontracting clause etc.
- Regular review of data processing activities is needed.

Kellerhals Carrard

Virginie A. Rodieux

Attorney-at-law, LL.M. | Senior Associate

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

virginie.rodieux@kellerhals-carrard.ch