Inno4Sports
Interreg Europe

European Union
European Regional
Development Fund

Inno4Sports Pilot Action

O1.2

Guidelines document about legal aspects of Data Driven Innovation

Cluster Sports and Technology
August, 2021

Table of content

1 Introduction

1.1 The Interreg Europe project Inno4Sports

The Interreg Europe project Inno4Sports brings together five regions (Hajdú-Bihar (HU), Lapland (FI), Lodzkie Region (PL), South Netherlands (NL) and Valencian Region (ES)) that all share the ambition to address a common objective, namely to strengthen the regional innovation ecosystems on sports & vitality based on market chances, social trends and business opportunities. The project started in 2018 and is now in the second phase.

In the first phase the participating regions have learned from each other's approaches, activities and good practises and from there developed regional action plans.
In the second phase of the project, each region is implementing its regional action plan. Besides the implementation of the action plans, 2 extra activities have started within the second phase:

1. 3 Regions (Lapland region, South Netherlands and Valencia region started a pilot action on the use of data in innovation activities for the sports & vitality domains
2. All project partners have adopted an extra activity to exchange Good Practices on how to deal with the challenges and new realities on innovation in sports & vitality that emerged because of the Covid pandemic.

This report describes activities in the pilot action in Phase 2, namely an introduction on the legal aspects on data driven innovation (DDI). It is a deliverable of the pilot action in Phase 2 of the project, but all project partners are invited to read this report, as it helps understand what are the possibilities but also the limitations on the use of (public and private) data in innovation activities.
GDPR regulations have been implemented in the EU society for the past years. It is important to understand the background and the purpose of these regulations in order to understand its implications in data driven innovation (DDI). It does not mean that the use of public data in new innovation opportunities is prohibited, but certain procedures need to be followed in order to comply with the regulations and, more important, to protect citizens against abuse of their own information. We therefore invite you to take good notice of the content of this report.

1.2 The use of (public and private) data in innovation processes

In the Inno4sports project, during the Interregional Event combined with Knowledge Capitalisation Seminar in Eindhoven (June 11-13, 2019), the regions Valencia (VLC) and Lapland (LPL) learnt through the presentations on June 12 about the Vitality Living Lab project (co-funded by ERDF South Netherlands Operational Programme, see GP South Netherlands), that the use of public sports data can have a significant impact on the development of sport products and services. Specially inspiring were the talks Vitality Data by Loes van Renswouw; TU Eindhoven; and #040 Beweegt! by Harmen Bijsterbosch, InnoSportLab Sport en Beweeg!, and the Municipality of Eindhoven (Innovation & Vitality in de Genneper Parken: Mikke Leenders, City of Eindhoven.

In these cases, public data amongst other socio geographic parameters (like health status, income, education, but also sports activities and memberships) are connected with activity parameters

(derived from e.g. Strava, an app that monitors cycling and running activities) and more infrastructural data (like roads, light paths, etc.). This gives insight in locations where people perform sportive activities, but also where boundaries are created by roads, bad illuminated paths and other factors that can be influence by (local) governments. As such these combinations of public data give insights for local governments to act upon and is defined as a Good Practise from South Netherlands (SN).

This represents a new approach called sport data driven innovation (DDI) and is seen by Valencia (VLC) and Lapland (LPL) as a driver of innovation and socioeconomic development. The pilot aims at testing this approach in different regional contexts.

During the pilot South Netherlands will provide the baseline methodological umbrella, context and support for the use of public data in innovation processes to the pilot. One important step in this is to transfer the knowledge on the possibilities and limitations of using (public) data and information in the context of GDPR regulations. This report deals with the content of a workshop that was held in June 2021 in order to transfer this knowledge.

1.3 Privacy and GDPR regulations

This report contains the information that was given during a dedicated workshop on Privacy and GDPR regulations, held on June 30, 2021 by Mrs Colette Cuijpers, Associated Professor Law & Technology of the Tilburg Law School, Tilburg University. The report will follow also the line of presentation during this workshop.

The report will describe both theory and practise in the following chapters:

- What is privacy?
- What is data protection?
- How do privacy and data protection relate?
- The privacy test of Art. 8 ECHR The basic principles of the GDPR
- Practice: Application to submitted cases/questions from the participating partners,

Finally, a reference will be given to the video that captured the workshop given on June 30, 2021

2 What is privacy?

When is there an infringement of privacy?

- Unjustified intrusion upon the private sphere of a natural person.

However, justification can come from the law or an overriding interest.

Privacy is not absolute: the right can be limited by law or can be overridden by legitimate interests of others, e.g. freedom of speech. Privacy is objective: everyone has the right to privacy. But how we experience or value privacy can be very subjective. What is private to one person, the other posts on social media for the world to know, e.g. sexual or political preference.

Privacy is described in Art. 8 ECHR – European Convention on Human Rights

ARTICLE 8 - Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence. (objective)
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. (not absolute)

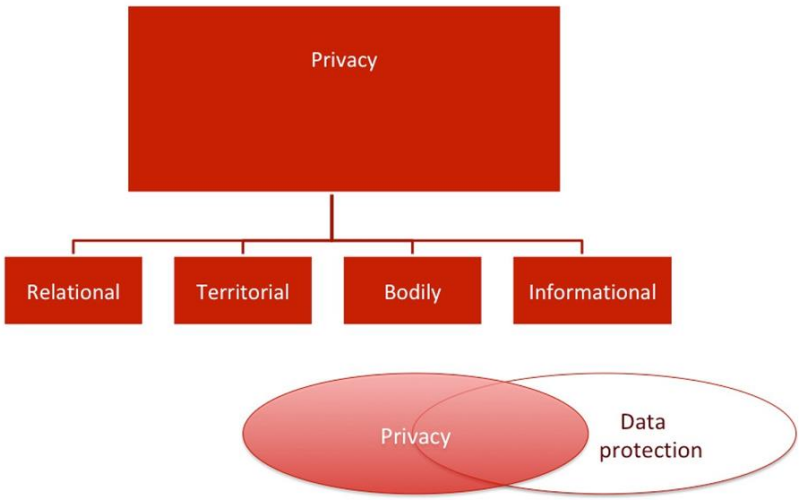
Privacy test of Art. 8

1. Is there an infringement of privacy?
2. Is the infringement foreseen by law? E.g. a law that indicates the authority to check people at airports in view of safety and security.
3. In the interest of one of the grounds listed in art. 8 (2) ECHR?
   e.g. in the example above national security and public safety.
4. Is the infringement necessary in a democratic society?
   a. proportionality?
   b. subsidiarity?

Figure 1. Examples of privacy and privacy infringement.[1]

[1] Sources: www.flashphoto.nl; http://travel.aol.co.uk/; http://www.pinkcatshop.com/; https://www.loesje.nl/posters/nl1210_0/; http://www.socialmediatoday.com

2.1 Relation of privacy and data protection



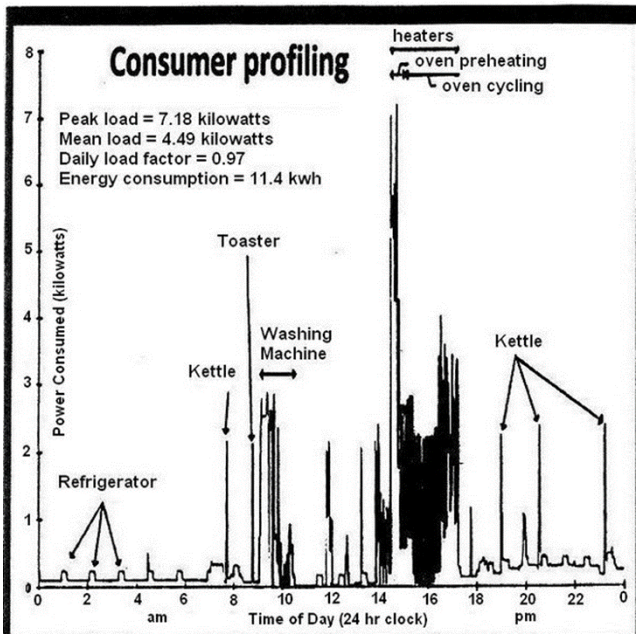
Art. 8 ECHR GDPR

Privacy can be a broader notion than data protection: it encompasses several dimensions including data protection, but also spaces (home/office), body and relations.

But privacy can be a more narrow concept than data protection: privacy only relates to the private sphere. Data Protection Rules apply always when processing personal data, also when the private sphere is not at stake.

Example: smart metering system

Based on measured data of energy consumption an activity profile could be determined.



Source: https://michiganstopsmartmeters.com/detailed-usage-reporting/

2.2 Privacy principles (FIP)

Source: https://www.cheatography.com/davidpol/cheat-sheets/oecd-privacy-principles/

These above mentioned principles are referred to as privacy principles, but are in fact Fair Information Practices and also known as such.

Meaning of Fair Information Practices:

1. Purpose specification – You must in advance specify the purpose for which you process personal data
2. Collection Limitation – You may not collect more data than necessary for the specified purpose
3. Use limitation – you may only use the data for that purpose
4. Data Quality – the data need to be accurate and relevant
5. Security – the data need to be secured
6. Openness – You must be transparent about your data processing
7. Accountability – and you need to be 'accountable' – demonstrate compliance
8. Participatory rights – you need to operationalise the rights of data subjects such as the right to erase and rectify data

These principles are the basis for the DPD and GDPR.

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995, p. 31–50
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 https://eur-lex.europa.eu/

3 Characteristics and structure GDPR

GDPR applies to public and private actors (specific regime for law enforcement).
The relation of GDPR to other specific laws is defined as follows: "lex specialis derogat legi generali" (more specific regimes supersede the GDPR, but must be compliant with the GDPR).
Lawfulness regime: Only processing that complies with the GDPR is allowed, otherwise forbidden. Non-compliance regardless of harm constitutes a risk (just like traffic rules). So not: unlawfulness regime = processing is allowed until damage is caused.
The GDPR law has a layered structure:

Layer 1: general – processing of personal data
Layer 2: special categories of data
Layer 3: transfer to third countries
(Layer 4: specific legislation)
(Layer 5: underlying legal relationship, e.g. employment contract)

And there is a focus on accountability, enforcement and fines.

3.1 Layer 1 of GDPR: the basis

The first question to pose when you start processing data is: when is the GDPR applicable?
Material scope (Art. 2 GDPR)
This regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
Territorial scope (Art. 3 GDPR)

1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

To answer the first question you need to pose some other questions:

- What does the GDPR terminology mean?
- When is there "processing of personal data"?

Definitions (Art. 4 GDPR)
(1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one 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;

Broad interpretation:

Recital 26: all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.

(2) 'processing' means 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;

In all those cases the GDPR is applicable.

The next question is: To whom is the GDPR applicable, which roles can be identified in the process of personal data processing? The roles are defined as: **controller** and **processor**

(7) '**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

(8) '**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The next question is: Which rights and obligations stem from the GDPR?

Key provisions: **Art. 5 and 6 GDPR**.

CHAPTER II

Principles

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 6

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Consent

(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Art. 7 More specific provision on consent

Art. 8 Consent from children – parents or guardians

Consent is not always the best ground for processing and it is better to use it as a 'last resort'. In stead it is better to use methods that avoid processing personal data, in particular in the case of children.

The rights of data subjects re defined in the following articles (corresponding obligations of controllers- operationalise – technical and organisational)

- Information and access (**Art. 12 and 15 GDPR**)
- Right to rectification (**Art. 16 GDPR**)
- Right to erasure (to be forgotten) (**Art. 17 GDPR**)
- Right to restriction of processing (**Art. 18 GDPR**)
- Right to data portability (**Art. 20 GDPR**)
- Right to object (**Art. 21 GDPR**)
- Right not to be subject to a decision based solely on automated processing, including profiling (**Art. 22 GDPR**)

Union or Member State laws can restrict these rights (Art. 23 GDPR).

Obligations towards controller and processor: the GDPR has more obligations that also pertain to processors:

- Not always easy to distinguish controller and processor
- Better protection to data subjects: data subjects can go to both the controller and the processor in case of issues with their data being processed.
- Information obligations (**Art. 12 – 15 GDPR**)
- Security obligations (**Art. 32 GDPR**)
- Notification data breach (**Art. 33 and 34 GDPR**)
- Data Protection Impact Assessment and Data Protection Officer (**Art. 35 and 37 GDPR**)

Obligations for processors

A processor needs to have an appointment of representative in the EU, and issue notification in case of data breaches, security, record of processing, DPO, cooperation with DPA (**art. 27 – 32, 37 GDPR**)

Art. 28 (3) GDPR:

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that **Art. 28 (1) GDPR**: a controller is responsible for the processor: Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

3.2 Layer 2 of GDPR: special categories of data

In Layer 1 we have considered the provisions pertaining to the processing of personal data. The next question to pose is are there special categories of data being processed. What are special categories of personal data?

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

After having considered the processing of personal data and special categories of personal data, the next topic is the transfer of data to third countries.

3.3 Layer 3 of GDPR: Transfer to third countries

In the third layer we need to consider if there is a transfer of personal data to third countries. And if these countries have an adequate level of protection. Which other grounds could be used to transfer the data?

Instruments for transfers of data to third countries are found in (**Art. 44 – 50 GDPR**)

Adequacy decision EC (**Art. 45 GDPR**)

Appropriate safeguards: Binding Corporate Rules (BCRs) **art. 46 and 47 GDPR**

Approved (by EC or DPA) standard contractual clauses (SCCs) **art. 46 GDPR**

Schrems I and II

Are we done now? No… Layer 4 and 5 still exist.

- Is there other relevant legislation?
- Is there an underlying legal relationship that is relevant?

3.4 Key focus of GDPR: Accountability

For any party processing personal data it is important to ensure and demonstrate compliance. In practice, parties experience this as burdensome and bureaucratic:

- Extensive information obligations (**art. 14 and 15 GDPR**)
- Keeping of a record of processing activities (**art. 30 GDPR**)
- DPO (**art. 37-39 GDPR**)

One important factor is the Data Protection Impact Assessment (DPIA): What are the risks of data processing and how can these be mitigated? (**Art. 35 GDPR**).

An answer can be given by Privacy by Design and by Default (PbDD) **Art. 25 GDPR**: "Built privacy into the design of the product or service"

Supervision is regulated by

- DPO (**Art. 37 – 39 GDPR**)
- Supervisory Authorities (DPAs) (**Art. 51 - 59 GDPR**)
- More cooperation DPAs (**Art. 60 - 67 GDPR**)
- European Data Protection Board (**Art. 68 - 76 GDPR**) (First: Article 29 Working party, many opinions still relevant)
- European Court of Justice (preliminary questions) such as: Schrems: Annulment Safe Harbour/Privacy Shield

See also http://curia.europa.eu/juris

In cases that parties do not comply to the regulations the Supervision bodies can issue fines as defined in the article on Administrative Fines (**Art. 83 GDPR**):

- 10 000 000 euro or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
- 20 000 000 euro or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

Figure: Privacy and data protection[2]

So it is very relevant to consider all steps in the GDPR regulations in order to avoid fining.

[2] Sources: http://blog.amadeusconsulting.com/importance-designing-medicalsoftware/; http://www.hipaacartoons.com/privacy-cartoons/

4 GDPR in summary

In summary if parties wish to use personal data for processing in either public or private activities it is important to check if GDPR regulations are applicable and if so, to take sufficient measures to avoid breaching the regulations.

Below there is an overview of relevant questions to answer when checking these GDPR principles:

1. Is the GDPR applicable?
    a. Is there processing of personal data?
    b. For an establishment in Europe or regarding EU citizens?
2. To whom does the GDPR apply?
    a. What is the division of roles: controller - processor?
    b. What is my role in the data processing?
3. Which rights and obligations stem from the GDPR?
    a. What is the purpose and ground for processing?
    b. Do I adhere to the Fair Information Practices?
    c. Accountability in order?
    d. Do I need to perform a DPIA?
    e. Do I need to appoint a DPO?
    f. What PbDD measures can I take?
4. Am I processing special categories of data? On the basis of which ground?
5. Are personal data transferred to third countries? On which ground?
6. Other relevant legislation or underlying legal relationship?

If these questions are answered satisfactory (and the answers are traceable) the GDPR principles have been followed.

5 Use cases

During the workshop specific use cases were brought in by the partners to see if GDPR regulations apply and if so, what measures should be taken in order to avoid breaching of the (principles of the) regulation. The following cases were dealt with.

5.1 Valencia Use case 1

1.- We are developing an online system for emotional evaluation of products and experiences. People see at the PC, or tablet, images or videos. During that, the user is recorded using his/her webcam. Image and natural language analysis are then used for eyetracking, expression recognition, comments analysis,...

5.2 Valencia Use case 2

2.- Persona digital twin for personalized services. For example, my knee injury risk. It is estimated from data registered with IOT, which is sent to a biomechanical model that estimates some parameters afterwards used for estimating the injury risk.

Additional remark relating to case 1 and 2

In both cases, we are including users to give specific consent for data use... but it is not sure if that is enough. Also, for case 1, when we integrate the system in the web of a company (a hotel for instance), the company starts getting afraid of that including an extra agreement to the user could reduce the possibility of the user staying at the website and purchasing something. In those cases, we are working on ideas about offering something extra to the visitor for agreeing with being recorded and so on. The question is if this approach complies with GDPR regulations.

5.3 Lapland Use cases

Regarding the upcoming GDPR Workshop and the relevant areas we require elaboration on regarding GDPR regulations: development of a sport hub learning and testing environment that will produce and analyse participants data. In this case further understanding regarding consent, usage and storage of this data would be valuable.

The feedback on these use cases can be found in the capture of the workshop (see annex 1).
Also more background and practical solutions for specific use cases can be found in the following literature: 'Privacy design strategies' by the author Jaap Henk Hoepman, see also https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

6 Annexes

6.1 Annex I

The capture of the workshop can be found on:
https://www.dropbox.com/s/yz7p02rgviaao85/210630%20GDPR%20Workshop%20Inno4Sports%20Pilot%20Action.mp4?dl=0