
POLICY FOR THE COLLECTING, PROCESSING AND SHARING OF DATA BETWEEN AFFILIATED NATIONAL FEDERATIONS AND THE UCI

The present policy (hereinafter: “the Policy”) aims at defining the relationship between the Union Cycliste Internationale (UCI) and its affiliated National Federations in regard to the Collecting, Processing and Sharing of Data.

The Policy forms an integral part of the UCI Regulations and National Federations undertake to reproduce the Policy in their respective regulations and abide by the Policy at all times when Collecting, Processing and Sharing Data.

1. DEFINITIONS

1.1. Unless the context otherwise requires, the following terms in the present Policy shall have the following meaning:

“Applicable Data Protection Law” shall mean the Swiss Federal Act on Data Protection (hereinafter the “FADP”) and its ordinances, as well as where and when any other applicable legislation in particular the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the “GDPR”).

“Controller”, “Processor”, “Data subject”, “Personal data”, “Collecting”, “Processing” (and “Process”), “Sharing” shall have the meanings given in the Applicable Data Protection Law.

“Data” shall be understood as a general term covering both “Personal Data” and “Sensitive Data” as defined hereinafter.

“Data Protection Authority” shall mean the relevant data protection authority in the territories where the UCI and the National Federations are established. In the case of the UCI, the Data Protection Authority is the Federal Data Protection and Information Commissioner (FDPIC) in Bern (Switzerland).

“Licence-holders” shall mean any individual who has been delivered a licence by a National Federation in the sense of Part I of the UCI Regulations.

“National Federations” shall refer to the members of the UCI accepted by the UCI Congress as being the representative organisations for the sport of cycling in their respective countries.

“Personal Data” shall have the meanings given in the Applicable Data Protection Law and includes personal data which may be collected and processed by National Federations and/or the UCI such as the surname, first name and maiden name; birth date; nationality; passport copy; gender; main address; email address; phone number; social media accounts; bank details; levels and categories; results; rankings; UCI ID; National Federation which delivered the licence and licence number; personal data of health professional or any person collaborating with a licence-holder.

“Security Breach” shall mean any unauthorized and/or unlawful Processing of, including access to, Data whether in electronic or hard-copy or other form, or interference with an information system, that compromises the privacy, security, confidentiality or integrity of Data.

“Sensitive Data” shall have the meanings given in the Applicable Data Protection Law and includes certain sensitive data which may be collected and processed by National Federations and/or the UCI specifically in the context of antidoping and paracycling such as medical data; whereabouts information; Therapeutic Use Exemptions (TUE); medical data contained in the biological passport; physical impairment; cause for the physical impairment; history and evolution of the physical impairment; general health condition; blood group; medical certificates; medical treatments; other medical condition; identity and details of the main doctor.

“Relationship of the parties” shall refer to the relationship between the UCI and National Federations.

“Shared Data” shall mean the Data which are collected by National Federations for the UCI.

“UCI” shall refer to the Union Cycliste Internationale which is the worldwide governing body for cycling.

2. SCOPE

- 2.1. As the worldwide governing body for cycling, the UCI collects, stores, shares and processes Data of Licence-holders and other individuals for the purposes of administration and governance, including the management of results and rankings, as well as in relation to anti-doping activities and the prevention of the manipulation of competitions, such as described in the UCI Policy on Data Protection available on the UCI website.
- 2.2. National Federations collect, store, share and process Data of Licence-holders as well as of other individuals for the purpose of their own activities. National Federations act as independent Controllers when Processing Data which are not shared with the UCI at the request of the UCI. However, National Federations shall comply at all times with the Applicable Data Protection Law and principles, as set out in section 3 of the present Policy.

2.3. Section 4 of the present Policy only applies to the Processing and Sharing of Data between National Federations and the UCI.

2.4. In this regard, National Federations act as Processors and shall comply with the obligations as set out in the UCI Regulations and in section 4 hereinafter.

3. NATIONAL FEDERATIONS' OBLIGATIONS AS DATA CONTROLLERS

3.1. In all cases, including when Processing Data as a Controller, National Federations undertake to respect the following principles:

- (a) Process Data lawfully, fairly and in a transparent manner in relation to Data of Licence-holders (lawfulness, fairness and transparency);
- (b) Collect Data for a specified, explicit and legitimate purpose and not further process Data in a manner that is incompatible with those purposes (purpose limitation);
- (c) Processing shall be adequate, relevant and limited to what is necessary in relation to the purposes to which they are processed (data minimisation);
- (d) Keep Data accurate and where necessary up to date (accuracy);
- (e) Keep Data in a form which permits identification of Licence-holders for no longer than is necessary for the purpose for which Data are processed (storage limitation);
- (f) Process Data in a manner that ensures appropriate security of the Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures (integrity and confidentiality);
- (g) Be responsible for and be able to demonstrate compliance with Applicable Data protection law (accountability).

3.2. When Processing Data which are not shared with the UCI, National Federations undertake to inform the UCI as soon as reasonably possible and as legally permitted:

- (a) In the event of a Security Breach;
- (b) In the event of a Data Protection Authority audit or investigation;
- (c) Any event that could potentially affect the UCI's liability or reputation.

4. NATIONAL FEDERATIONS' OBLIGATIONS AS DATA PROCESSORS

4.1. Pursuant to the UCI Regulations, licences are issued by the National Federation of the country where the licence-holder has his main residence at the time of application.

- 4.2. Licence-holders' Personal Data are collected for the UCI by National Federations by means of the licence application form contained in articles 1.1.021 and 1.1.022 of the UCI Regulations, which represent the instruction of the UCI.
- 4.3. Licence-holders' Sensitive Data may be collected either by the UCI or by National Federations through specific processes put in place to this effect.
- 4.4. When Processing Data for the UCI, National Federations shall ensure that:
- (a) Data are processed only in accordance with the Applicable Data Protection Law and the written instructions of the UCI, in particular this section 4;
 - (b) Licence-holders have been provided with the relevant information regarding the scope of Collection, Processing and Sharing of their Data and informed of their rights to consult or to request access, rectification or deletion of their Data, including information mentioned in section 4.5;
 - (c) Licence-holders have freely consented to the Collection, Processing, and Sharing of their Data by filling-in the licence application form after having been properly informed;
 - (d) Data is only processed for the UCI and not for National Federations own interest¹;
 - (e) Any individual or entity that is authorised to access Licence-holders' Data (including staff and subcontractors) shall be subject to a strict duty of confidentiality (whether contractual or statutory) and shall not permit any individual or entity who is not under such a duty of confidentiality to process the Data;
 - (f) Data are secured at all times, in particular by implementing and maintaining at National Federations' costs and expenses appropriate technical and organisational measures to protect Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to. National Federations shall also ensure that an efficient protocol is in place in the event of a Security Breach, at least as set out in the Applicable Data Protection Law;
 - (g) Data are accurate. In this regard, National Federations shall take reasonable steps to ensure that such Data remain accurate on an ongoing basis, informing the UCI within a reasonable deadline of any updates or corrections to the Data;
 - (h) All the necessary measures are taken in case of an international transfer of Licence-holders' Data to ensure that the transfer complies with Applicable Data Protection Law. National Federations shall take specific care when transferring Licence-holders' Data to

¹ A processing in the interest of a National Federation is only possible when it acts as a Controller.

Recipients located outside of Switzerland and the European Economic Area (“EEA”) where applicable standards may be different;

- (i) The UCI will be immediately informed if National Federations consider that an operation infringes an Applicable Data Protection Law;
- (j) All Data will be returned or erased when they are no longer necessary;
- (k) The UCI will be immediately informed of any request of a Licence-holders or Data Protection Authorities;
- (l) Another processor will not be engaged without the prior written authorisation of the UCI. In the case of a general authorisation, the National Federation shall inform the UCI of any intended changes concerning the addition or replacement of other processors, thereby giving the UCI the opportunity to object to such changes;
- (m) National Federations will assist the UCI in ensuring compliance with the obligations pursuant to Applicable Data Protection Law, including with the notification of a Security Breach, the answer to Data Protection Authorities and Licence-holder’s requests, data protection impact assessments and the demonstration of its compliance.

4.5. National Federations are aware and accept that the UCI may transfer the Shared Data when necessary for administration and governance purposes to entities and individuals such as other National Federations; the International Olympic Committee (IOC); the World Anti-Doping Agency (WADA); National Anti-Doping Organisations (NADO); the Cycling Anti-Doping Foundation (CADF); the Court of Arbitration for Sport (CAS); the judicial bodies of the UCI; national and international authorities competent in relation to investigations and/or procedures in relation to potential violations of the UCI Regulations and any other processing operation of personal information that is legitimate and proportionate in the context of the administration and governance of cycling; event organisers; companies in charge of timing on UCI events; companies in charge of delivering accreditations on UCI events; companies contracted by the UCI for the management of its servers and databases; companies in charge of online registration to UCI events; UCI legal counsels; scientific experts; UCI officials such as Commissaires and Classifiers.

4.6. National Federations are responsible to inform the License-holders before the collection of Data.

4.7. The above-mentioned obligations also apply when National Federations process Data for the UCI relating to individuals who are involved in the sport of cycling but who do not necessarily hold a licence.

5. COMMON OBLIGATIONS OF NATIONAL FEDERATIONS AND THE UCI

- 5.1. Upon request, the UCI and National Federations undertake to comply and collaborate fully with the Data Protection Authority.
- 5.2. The UCI and National Federations shall prevent from doing and/or permitting anything to be done by act or omission that would be contrary to Applicable Data Protection Laws and/or cause any liability under Applicable Data Protection Laws.