

GDPR4 CHILDRN

Processing of personal data in hobbies

A Guide for the board of the association



Contents

Data protection icons	3
Why is the protection of personal data important?	5
1. Privacy is a fundamental right	5
2. Sensitive personal data requires particularly careful protection	8
3. Personal identity codes may only be processed if necessary	10
What roles are involved in processing?	11
1. The controller is responsible for the processing of personal data	12
What principles must be observed in the processing of personal data?	15
2. Processing requires a basis	17
2.1 Legal bases for processing personal data	17
2.2 Consent requires an indication of the participant's wishes	19
2.3 Consent from minors	20
3. Only use personal data for the planned purposes	22
4. Inform data subjects transparently of the processing of personal data	24
5. Only process necessary personal data	27
6. Only process accurate personal data and rectify inaccurate data	29
7. Ensure the security of processing	30
8. Define storage periods for personal data and erase unnecessary data	32
8.1. Storage period	32
8.2. Storage location	33
8.3. Erasure	33
9. Demonstrate compliance with data protection legislation	36

What obligations does a hobby organiser have in the processing of personal data?	37
1. Fulfil the participants' data protection rights	37
2. Describe the hobby organiser's processing of personal data with a record of processing activities	41
3. Agree on processing	43
4. Assess the risks and impact of processing	44
5. Report personal data breaches	46
6. Only transfer personal data out of the EU if the conditions are met	50
7. Give people involved in the hobby instructions and training in data protection	52
8. Manage the life cycle of personal data from planning to collection, storage and erasure	54
What should you take into account when publishing photos and videos?	57
What should you take into account when processing health data in hobby activities?	59
What should you take into account when disclosing personal data in hobby activities?	61
ANNEX 1: CONSENT FORM – TEMPLATE	63
ANNEX 2: COMICS TO INFORM ABOUT DATA PROTECTION	64

Data protection icons

In the guide, you will find icons shown below. They provide information on data protection in a visual form. Associations are free to use these icons, for example, in their own communications.

Read more about the icons: [Data protection Icons](#) | [Data protection in hobbies](#).¹



**DATA
PROTECTION**

Data protection legislation determines how personal data can be processed in hobby activities. Among other things, the controller has an obligation to process personal data with care and inform data subjects transparently about such processing.



CONTROLLER

The party that determines for what purposes and how personal data is being processed in hobby activities is the controller. In hobby activities, the party responsible for the processing of personal data is generally the controller of the personal data.



DATA SUBJECT

The data subject is the person to whom the personal data relates. In hobbies, those participating in the hobby and their custodians can be data subjects. Data subjects have data protection rights, such as the right to access personal data concerning themselves.



**CHILDREN'S
PERSONAL DATA**

Children's personal data must be protected carefully, and children should be informed of the processing of their personal data in child-appropriate terms.

¹ <https://tietosuojaharrastuksissa.fi/en/material-bank/data-protection-icons/>



**SENSITIVE
DATA**

Special categories of personal data or sensitive data include health data and information revealing a person's ethnic origin or religious beliefs.



**PERSONAL DATA
BREACH**

A personal data breach means an incident that results in, for example, the destruction or loss of personal data, or that grants a party not authorised to process the data, access to the personal data.



Why is the protection of personal data important?

1. Privacy is a fundamental right



Privacy is a fundamental right. Children, young people and their parents must be able to feel secure that the law is being followed in the processing of their personal data also in hobby activities. The hobby organiser has an important role in ensuring data protection and establishing good practices. When data protection is in order, everyone can focus on the hobby and rest assured that their personal data are in good hands.



What does data protection mean?

Data protection safeguards the right to privacy. Data protection is a fundamental right that safeguards the rights and freedoms of people in the processing of personal data. Data protection also aims to prevent damage from the inappropriate processing of personal data to the people whose personal data are being processed in the hobby activities.

What are personal data?

Personal data refers to all data related to an identified or identifiable person. Directly identifiable personal data include the personal identity code, uncommon names, and photographs featuring the person, while people can be identified indirectly from data such as their address and date of birth. Combining different data can result in personal data if the individual can be identified from the combined data.

What does data protection legislation mean?

Data protection legislation sets the framework for when and how personal data can be processed. The hobby organiser must take the requirements of data protection legislation into account in its activities when processing various kinds of personal data.

Data protection legislation consists of the EU General Data Protection Regulation (EU 2016/679), Finland's national Data Protection Act (1050/2018), and special legislation providing for matters such as processing patient records or the personal data of employees.

Many kinds of personal data, such as names, personal identity codes, addresses, allergy information, bank account numbers, dates of birth, photographs and videos are processed in hobby activities. Personal data processed in hobbies can include the data of participants and their custodians, employees, volunteers, instructors, coaches and Board members. Such processing includes the collection, use, viewing, transfer, disclosure and storage of personal data.

Everyone involved in hobby activities plays an important role in ensuring compliance with data protection requirements, since many stages of hobby activities involve the processing of personal data in one way or another. Depending on the hobby, personal data can be processed in connection with registering for camps, organising competitions, paying licence fees, and informing members about practice schedules. Personal data can be processed in various electronic systems, on paper, or with a variety of technical devices, such as smart phones and computers.

The hobby organiser must take the nature of the activity into account when choosing processing methods. For example, personal data may have to be processed on paper during a scouts' hike in the woods, when access to electronic personal data is limited, in which case the organiser has to comply with the requirements for processing personal data on paper.



Who is a data subject?

The data subject is the person to whom the personal data relates. In hobbies, data subjects include club members, Board members, club employees, volunteers, team managers and the custodians of club members.

Why must the hobby organiser comply with data protection legislation?

Compliance with data protection legislation is just as mandatory as following any other law, for example when doing your club's accounts. When processing is meticulous and legal, the hobby activities run smoothly, personal data are accurate and up to date, decisions are based on correct information, and emails get sent to the right addresses. When that is the case, the participants can also rest easy knowing that the hobby organiser is complying with the law.

Neglecting data protection can cause financial losses, reputation damage and unnecessary work to the hobby organiser. Trust in the hobby organiser can suffer if people are not sure what their personal data is being used for or who it is being disclosed to. Shortcomings in processing can cause reputation damage and financial losses to club members as well.

Data protection rights apply to every child and young person too. When a hobby activity is being organised for children, the organiser must remember that it is processing the personal data of children. Children's personal data must be protected especially carefully, because children are not always aware of the risks and consequences of processing or of their rights and ways of safeguarding their data.



Remember

Identify what personal data is being processed in your hobby activities and by whom. Do not collect personal data "just in case".

The purpose and rules of the hobby organiser's (such as a sports club, craft club or scout troop) activities determine which personal data it needs to collect from participants. The hobby organiser must evaluate the necessity of each item of personal data being collected. It must be able to demonstrate that all personal data collected are necessary for its activities. Personal data may not be collected "just in case", but only in a planned manner and for purposes defined in advance.

2. Sensitive personal data requires particularly careful protection



'Special categories of personal data' include sensitive information indicating the person's ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health status, sexual orientation or sex life, as well as genetic and biometric data. As a rule, the processing of such personal data is prohibited. Such data may only be processed on special grounds and with special care.

Hobby organisers may process data about a person's

- health,
- religious or philosophical beliefs,
- ethnic origin,
- political opinions,
- sex life and sexual orientation, and
- trade union membership.

Sensitive data must be protected especially well. The processing of special categories of personal data is only allowed on specific grounds laid down in the GDPR or other legislation. Hobby organisers can process such data on the following grounds:

1. The data can be processed with the person's informed and unambiguous consent. Explicit consent can be given by means such as signing a written statement, or with an electronic signature or two-factor authentication. For example, the person can first reply to an email sent by the hobby organiser, after which an electronic confirmation link or code will be sent to them.
2. A political, philosophical or religious association or other non-profit organisation can process special categories of personal data when all of the following requirements are met:
 - The data is being processed in connection with the organiser's legal activities.
 - The data is appropriately protected (e.g. technical safeguards, access rights management and password protection).
 - The organisation is only processing the data of its members, former members or individuals with a close connection to the organisation.
 - Data is not disclosed to outside parties without the person's consent.



What do hobby organisers need to take into account when processing sensitive personal data?

1. Identify the special categories of personal data being processed in your hobby activities and make sure that it is necessary to process them.
2. Make sure that the hobby organiser has special grounds for processing the data. For example, the processing of a participant's allergy information during a scout camp in the woods could be based on the participant's specific consent. If sensitive data is being processed on the basis of the person's consent, you need to be able to demonstrate that the consent has been given.
3. Make sure that special categories of personal data are well protected, for example with technical safeguards, access rights management and password protection.
4. Specify the individuals whose duties include the processing of special categories of personal data in the hobby activity. Make sure that only the people whose duties include the processing of sensitive data have access to the data, and that those people are aware of the special requirements related to the processing of sensitive data.
5. Specify the storage period for the personal data. The storage period must reflect the purpose of the processing. For example, if information on the participants' allergies has only been collected for a scout camp in the woods, the data must be erased at the end of the camp.



Remember

Take special care to protect sensitive data. Make sure that you have special grounds for processing special categories of personal data.

3. Personal identity codes may only be processed if necessary

Personal identity codes may not be processed unnecessarily, so every hobby organiser needs to make sure that they have a basis for processing personal identity codes. The personal identity code is only used for identifying people and may not be used in training attendance lists or as a username, for example.

Processing personal identity codes in hobby activities can be justified if there is a need to identify individuals reliably and the identification cannot be achieved by other means. It is often possible to distinguish between individuals based on their dates or years of birth alone, in which case it is not necessary to process the complete personal identity code. The collection of personal data should always be minimised.

If you do decide to process personal identity codes, you need to know the purpose of the processing and whether it is permitted by law. Personal identity codes may only be processed with the data subject's consent or if the processing is provided for by law. The hobby organiser must assess the processing of personal identity codes on a case-by-case basis. It must also make sure that people who do not have the right to process personal identity codes do not have access to them and cannot see them by accident. If personal identity codes are being processed, the data file must be secured effectively. Personal identity codes must not be entered on documents printed out or drawn up on the basis of the data file unless necessary.



Remember

Only process personal identity codes in hobby activities if it is important to reliably identify participants in order to ensure the fulfilment of their rights and obligations, or for the performance of statutory duties.

What roles are involved in processing?

It is important for the hobby organiser to identify the parties processing personal data and their roles in that processing.



What does 'controller' mean?

The controller is the person or organisation who determines the purposes and means of processing personal data. In the context of hobby activities, the controller can be the sports club's board, because it is responsible for the club's activities and determines how personal data is processed in those activities and for what purposes.

What does 'joint controller' mean?

When the purposes and means of processing personal data are determined by two or more parties together, they are called 'joint controllers'. Joint controllers must agree on their responsibilities in a clear and transparent manner, for example by contract.

What does 'processor' mean?

The processor processes personal data on behalf of the controller, that is, according to the controller's instructions and under its direction. The processor often has access to the controller's personal data. An example of a processor would be a company providing various services, such as IT services, to the controller.

1. The controller is responsible for the processing of personal data



CONTROLLER

The party that determines for what purposes and how personal data is being processed in hobby activities is the controller. As a rule, the party responsible for the hobby activity is the controller of the personal data. It is the controller's duty to ensure that the processing of personal data complies with the data protection legislation.

The definition of 'controller' is functional: the purpose of the definition is to allocate responsibility for compliance with data protection regulations to the party that can actually influence the processing. When a hobby organiser uses an external service provider for managing the personal data of participants, an ERP system provided by an IT service provider, or an accounting firm for drawing up its accounts, the hobby organiser is the controller of the personal data processed by these external service providers, because it decided how and for what purposes the personal data is processed. In such cases, the external service provider is the processor. Even though the processor is processing the hobby organiser's personal data, as the controller, the hobby organiser remains responsible for the personal data.



Remember

The controller determines for which purposes personal data is processed and how.



Example

A gymnastics club processes the personal data of various people in its activities. It processes the club members' personal data for enabling hobby activities, the personal data of the club's coaches for the payment of wages, the data of contestants in gymnastics competitions organised by the club, as well as the personal data of representatives of the club's sponsors. The gymnastics club processes the club members' personal data in the SPLITS system provided by Sports Systems Inc.

The gymnastics club considers the club's Board to be the controller of the personal data processed in the club's activities, because the Board is responsible for the gymnastics club's activities and has determined the above-mentioned purposes and means for the processing of personal data in the hobby activity. The club's Board is also the controller of the personal data being processed in the SPLITS system even though Sports Systems Inc is providing the system to the gymnastics club, because the Board has determined how the data is to be processed and which club employees can process which data in the system. Sports Systems Inc Oy serves as the processor of the personal data contained in the system.

In this example the Gymnastics club Board is the controller

- determines why and how the personal data is processed

In this example Sports Systems Inc. is the processor

- processes personal data on behalf of the controller and according to its instructions

2. A processor acts on behalf of the controller

Even though the controller determines the purposes and means of processing personal data, it does not necessarily do all of the processing itself. A person or organisation processing personal data on behalf of and according to the instructions of the controller is called a 'processor' of personal data. For example, the provider of membership registry software acts as a processor on behalf of the hobby organiser.

The processor can be a company, private entrepreneur, authority, or association. Individual employees of the controller who process personal data as part of their duties are not processors in this sense.

Processors can include IT service providers with access to the controller's personal data. The duties of processors can be very specific, such as outsourced mail delivery. But they can also be broad in scope, such as managing a service for another organisation or the payment of salaries.

A processor may only process personal data for the purposes defined by the controller. It cannot start processing that data for its own purposes.

It is essential for the hobby organiser to identify the parties processing its personal data and ensure that a processing agreement has been signed with them. More information on the contents of a processing agreement is available in section "Agree on processing" on page 43.



Remember

The processor processes personal data on behalf of the controller and according to its instructions.



Example

A football club has purchased an application from IT provider Corner Kick Ltd in which its players register for training. Corner Kick Ltd has access to the players' and coaches' personal data in the application. Corner Kick Ltd provides the registration service through the application and processes the football club's personal data on behalf of the club and according to its instructions. Therefore, Corner Kick Ltd is the processor of the personal data processed in the registration app, and the football club is the controller.

What principles must be observed in the processing of personal data?



Data protection principles are general principles and practices applying to the processing of personal data. They are intended to guide processing.

According to the principles, personal data must be:

1. processed lawfully, appropriately and transparently
2. collected and processed for specified, explicit and legitimate purposes
3. collected only to the extent necessary for the purpose of the processing
4. updated whenever necessary: inaccurate personal data must be erased or rectified without delay
5. stored in an identifiable form only for as long as necessary
6. processed confidentially and securely

The data protection principles must be observed for the entire life cycle of processing, that is, from the collection of the data to its storage and erasure. The principles must be observed at all times and cannot be derogated from even with the data subject's consent.

1. Take data protection into account from the start and in all circumstances

Data protection should be the first consideration in all processing of personal data in hobby activities and should be automatically taken into account whenever processing is begun or processing practices change.

Data protection principles must be effectively integrated into all stages of all functions involving the processing of personal data. The hobby organiser must take the necessary measures to ensure and demonstrate compliance with data protection legislation. Such measures can include training, instructions and orders for employees, surveillance of premises, monitoring of the use of personal data, ensuring the security of information systems, encryption of data, technical restrictions, and audit and surveillance systems.

2. Processing requires a basis

The lawfulness of processing is one of the principles of data protection. It means that the processing of personal data always requires a basis in law.

The basis for processing must be chosen before the start of processing. Personal data can be processed on more than one basis. But after a basis has been specified for processing, it can no longer be changed. If there is no statutory basis for the processing of personal data, it is illegal. The processing basis affects things like the data protection rights available to the data subject.

2.1 Legal bases for processing personal data

Personal data can be processed lawfully on the following bases:

a. Consent of the data subject

A person can give their consent to the processing of their personal data for a specific purpose. Consent can be given in writing, verbally, or by another clear and affirmative act, such as ticking a box on a website. Withdrawing consent must be as easy as giving it. Read more about requesting a consent in the section "Consent requires an indication of the participant's wishes" on page 19.



Example

The instructor of a painting club gives the participants a paper form asking for their consent to taking photographs at the next meeting and for using the photographs to publicise the club's activities on its website.

b. Agreement

When the data subject is a party to an agreement, their personal data may be processed for the performance of the agreement. For example, if someone orders a supporter shirt from a sports club, the club is allowed to process their address information to deliver the order. It is important to define the precise contents and purpose of the agreement because the assessment of the necessity of processing will be based on them. Only necessary personal data may be processed.

c. Compliance with the controller's legal obligation

Compliance with the controller's legal obligations may require the controller to process personal data. Controllers operating in both the private and public sectors can be subject to legal obligations, which can only be based on EU law or national legislation.



Example

A hobby organiser reports the pay of its employee to the Tax Administration. Because tax legislation obliges the hobby organiser to declare its employees' pay to the Tax Administration, the basis for processing is compliance with the controller's legal obligation.

d. Safeguarding the vital interests of the data subject or another person

The processing of personal data is allowed when it is necessary to safeguard the vital interests of the data subject or another person. This processing basis is suitable in situations concerning life and death or threats that could result in injury to a person or otherwise be detrimental to health. The processing of personal data can serve a vital interest in a humanitarian crisis, such as during a natural disaster or epidemic. In such circumstances, processing could be required to track the spread of the epidemic, for example.

e. Performance of a task carried out in the public interest or the exercise of official authority vested in the controller

Personal data may be processed when required by the public interest or the exercise of the official authority vested in the controller. This can serve as a processing basis in both the private and public sectors when the public interest of the EU or the State is at stake or official authority is being exercised. The task in the public interest or official authority must have been vested in the controller by law or other legal provisions. For example, processing personal data for scientific or historical research or for the compilation of statistics can constitute processing in the public interest.

f. Legitimate interest

The processing of personal data is allowed when it is carried out for the legitimate interest of the controller or a third party. A 'balance test' can be conducted to determine whether an interest is legitimate. In the test, the interest of the controller or third party is balanced against the data subject's interests and fundamental rights. For example, the controller may have a legitimate interest for processing when the data subject is the controller's customer or subordinate.



On what basis can a hobby organiser process personal data?

In hobby activities, the processing of personal data can be based on the data subject's consent, legal obligations or the controller's legitimate interest.



Remember

Make sure that you have at least one of the six bases for processing personal data. Remember that you can have different bases for the processing of personal data for different purposes.

2.2 Consent requires an indication of the participant's wishes

Consent is one of the possible bases for the processing of personal data. Valid consent requires a

- specific,
- informed,
- freely given, and
- unambiguous statement.

The data subject can give their consent to a predefined, explicit and legal purpose of processing. If the purpose of processing the personal data changes, the controller must obtain the data subject's consent again before starting processing.

'Specific' consent means that the purpose for which the data is being collected must be specified when requesting the consent. In other words, separate consents must be requested for each purpose of processing, and it is not possible to request the data subject's consent to all kinds of processing of personal data in advance without specifying to what the data subject is giving their consent.

The consent must also be freely given. That is, the data subject must have a real opportunity to refuse their consent and also be able to withdraw their consent later without any negative consequences. Consent is not freely given if the data subject is in a vulnerable position in relation to the controller. The data subject can be in a vulnerable position if the controller is the data subject's employer, for example.

Consent must also be clear and unambiguous, so silence, inactivity or a pre-ticked box on a form are not indications of consent. For example, when a child registers for a sports club with an electronic form, the form cannot have a pre-ticked section requesting consent for publishing team photographs on the club's website or simply state that, by joining the team, the child automatically consents to the publication of their photographs.



Example

A sports club starts a trial, offering smart watches to its basketball team. The purpose is to monitor the players' recovery from exertion. The club distributes a form to the players, requesting their consent for the use of the smart watches and the processing of the data obtained with them. The form states that, if the player does not consent to the use of the smart watch, they will have to train with another team for the duration of the trial and will not be permitted to train with their own team.

A player would not like to participate in the trial, but feels pressured to do so because they want to train with their own team and may think that declining to participate could have negative effect on the club's trial. In this case, the player's consent is not freely given and does not meet the requirements set for consent.

2.3 Consent from minors



The special status of minors must be taken into consideration when requesting consent from them. When requesting consent, the controller should consider whether the underage participant is capable of understanding the effects of the processing of their personal data. The controller should also take into account the vulnerable position of underage participants in relation to the controller. If consent is being requested from a child, special attention must be paid to clear and plain language.

In case of offering social media and other applications directly to children, the child must be at least 13 to consent to the processing of their personal data. If the child is under 13, the consent or authorisation of their custodian is required for the processing of their personal data. There are no other age limits for requesting consent from children. Rather, the party requesting the consent must evaluate the child's capability to give their consent on a case-by-case basis in view of the purpose for which it is being requested.

If consent is requested directly from the child, it must be requested in a manner and in circumstances which permit the child to refuse without fear of consequences such as falling out of favour.

If the consent is being requested from the minor's custodian, the controller must determine which of the child's custodians is authorised to give their consent on the child's behalf. As a rule, children are represented by their custodians. But a child's parents are not always their custodians. If a child's parent is not their custodian, the parent may not have the right to represent the child in all respects or even have the right to access the child's information.

3. Only use personal data for the planned purposes

The principle of purpose limitation means that personal data may only be collected for specific, predefined purposes. The purpose of processing must be defined clearly in advance. Nor may the data be processed in a manner that is incompatible with those purposes later.

The data subjects must be informed of the purpose of processing their personal data. The purpose of the data must also be documented, i.e. written down. Only processing personal data for a specific purpose is a key factor in the maintenance of trust. Defining the purpose of processing helps the data subject

- understand what their data is needed for;
- evaluate whether the purpose is appropriate; and
- decide whether they want to influence the processing of their personal data by exercising their data protection rights (read more about data protection rights in section “Fulfil the participants' data protection rights” on page 37).



Example

A dance academy has determined that it processes personal data for the following purposes in its operations: maintaining the club's membership registry, arranging dancing classes, communicating about activities, collecting membership fees, delivering the club's newsletter, and paying salaries.

Personal data may be processed for new purposes if the planned purpose complies with data protection regulations and

- the data subject's consent for the new purpose is obtained before the start of processing,
- or
- there is a clear legal basis for the processing.

If the controller intends to process personal data for new purposes, it must notify the data subject of this before the start of processing. The controller must inform the data subject of the new purpose of processing, the rights of the data subject and all other necessary matters, unless it has a legal reason for derogating from the duty to inform.



Remember

Define a specific purpose for the processing of personal data and only process the data for that purpose. If you intend to use the data for other purposes as well, you need to notify the data subjects of the change in purpose before starting the processing.

4. Inform data subjects transparently of the processing of personal data

The transparency of processing personal data means that the controller must openly tell the data subjects how it is processing their personal data. The controller is required to provide all information concerning the processing of personal data to the data subjects in a concise, intelligible and clear form. The information does not have to be provided in a prescribed form.



Example

A music club has attached a description of how and why it is processing the club members' personal data to the electronic registration form for joining the club.

If the personal data will be collected directly from the data subject, the controller should inform them of the processing when collecting the data. If the personal data is not collected from the data subject themselves, they must be informed of the processing within a reasonable time and no later than one month from obtaining the data.

When data used for communicating with a person is obtained from another source than the person themselves, they must be informed when contacted for the first time, at the latest. If data intended for disclosure to another recipient is obtained from a source other than the data subject themselves, they must be informed of this before or in connection with the first disclosure.



Example

A sports club has drawn up a privacy statement of their processing. The statement is distributed to new members when they join the club. The privacy statement tells the data subjects on what grounds and for which purposes the sports club processes the personal data of its members, which personal data is being processed and for how long, as well as the data protection rights available to the club members.



When must participants be informed of the processing of personal data by the hobby organiser?

As a rule, a participant must be informed of the processing of their personal data when the processing begins. This can be done with a privacy statement on the hobby organiser's website, an information letter sent to every participant, or on the registration form for the hobby. The choice of method depends on how the personal data is processed.

The hobby organiser can also inform the participants and their custodians of the processing of their personal data at regular intervals, especially if changes are made to the processing.

When processing children's personal data, the controller should make sure to inform the children of it using language and style that the child can understand. In other words, it is important to describe the processing of personal data in a manner appropriate to the audience.

Read more: [Informing the data subject | Office of the Data Protection Ombudsman](#).²



Remember

Inform the parties involved in hobby activities (e.g. the participants, employees, instructors, coaches, custodians and stakeholders) of the processing of their personal data. Pay special attention to the intelligibility of information provided to children.

² <https://tietosuoja.fi/en/inform-data-subjects-about-processing>



Example

An ice hockey team is taking part in a skill training camp organised by the club. When the team registers for the camp, the club informs members how the personal data collected in connection with the registration is processed by the club. The club specifies the personal data collected and processed in connection with the registration (e.g. the name, contact details, and accommodation and dietary information of each team member). The club also states the purposes for which the data will be processed (e.g. for organising and coordinating the skill training camp), the basis for processing the data collected in connection with registration, as well as the storage period for the data. The ice hockey club also informs the participants of how they can exercise their data protection rights (for example by contacting the team's coach or sending email to the club's address designated for data protection issues).

5. Only process necessary personal data

Data minimisation is one of the principles of data protection. It means that the processing of personal data must be limited to what is necessary and the controller must be able to justify the need for processing the data. Data minimisation must be taken into account in all aspects of the hobby activity from the very beginning.

Data minimisation must be taken into account already when collecting data: information that is not necessary for the hobby activity may not be collected about participants, their custodians, or any other people involved in the hobby activity. To ensure that only the necessary personal data is collected, the controller must evaluate, on a case-by-case basis, the purposes for which the data is being collected and what data is necessary for those purposes. The storage of personal data must also be limited: personal data that is no longer necessary may not be stored for no reason.

When publishing information, you must make sure that you do not publish unnecessary information on your website or publish unnecessarily detailed information about participants on social media. When publishing information on the internet, on social media and in messaging applications, you should remember that the controller may not be able to control what happens to the personal data after publication. Limiting the processing of personal data to the strictly necessary helps prevent the uncontrolled spread and potential misuse of personal data.



Remember

Minimise the processing of personal data in hobby activities by considering carefully whether you have to process personal data and which data are necessary for which purpose.



Example

A sports club is organising a kick-off event for the autumn season at its home arena. The club asks participants to register for the event so that it can get the right number of merchandise gifts for the participants. On the registration form, the club only asks participants to indicate whether they will be attending the event or not, since it does not need to know the participant's name or other contact details in order to get the gift merchandise.



How can the hobby organiser take into account requirements such as data minimisation?

Before you begin processing personal data, you must determine whether processing is required for your intended purpose in the first place. If the processing of personal data is necessary, you need to evaluate which data will be necessary for the purpose.

If you intend to publish lists containing personal data either online or on paper on a notice board, you need to consider in advance whether it is actually necessary to publish the list at all. If publishing is necessary, you must evaluate whether the list contains any personal data that is not necessary to publish.

Example: A gymnastics club sends an email to a custodian who has registered their child for fairy-tale gymnastics, confirming that the child has been accepted into the group. The club does not publish the names of people who have registered their children for fairy-tale gymnastics online, because it informs everyone accepted into the group personally by email, thus minimising the publication of personal data on its website.

System access rights are limited so that only persons who are supposed to process personal data can access them.

The use of file-sharing services, for example for processing the personal data of football players on a large scale and to which all club members and their custodians have access, should be avoided.

When sending email to a large number of recipients, you can enter the recipients' email addresses in the BCC field so that the recipients cannot see everyone's email addresses.

Specify the methods and places for processing personal data in advance, so that the same data is not processed in several places unnecessarily.

You should avoid printing out personal data without a good reason, so that it is not disclosed to outsiders or stored unnecessarily.

6. Only process accurate personal data and rectify inaccurate data



DATA SUBJECT

The requirement of accuracy means that any personal data being processed must be accurate and up to date. Inaccurate personal data must be rectified or erased without delay.

The controller must ensure the accuracy of the personal data being held by it. Ensuring the accuracy of personal data is especially important when it is used to make decisions related to the data subject. Inaccurate data can sometimes have serious consequences. For example, a participant's health could be endangered if the provider of camp meals knows that they are allergic to apples but does not have information about the participant's nut allergy.

The controller must have methods for evaluating the accuracy of data on a regular basis and updating the data as required. Data subjects also normally have the right to request the rectification of inaccurate data and the erasure of unnecessary data.

If a controller obtains data from another controller, the source of the data should be written down in a comment attached to the data. If the data turns out to be inaccurate, this information can then be conveyed to the original controller as well.

When correcting personal data, make the changes everywhere it is being stored or processed. Collecting data directly from participants and asking them to notify the hobby organiser of any changes is a good way of ensuring the accuracy of personal data.



Example

A crafts club asks participants to tell the instructor about any changes in their contact details or other information.



Remember

Check the accuracy of participants' personal data regularly and rectify inaccurate data everywhere it is being stored. Ask participants to notify you of any changes to their data.

7. Ensure the security of processing



The hobby organiser must take care of the protection of data at all stages of processing from collection to erasure. Secure processing requires that the controller is able to guarantee the confidentiality, integrity, usability and resilience of the systems and services at all times and is able to restore the data quickly in the event of a fault. The processing of personal data must also be monitored and supervised to ensure security.

The adequate level of data security depends on the nature and volume of the data being processed. For example, sensitive data and special categories of personal data require more effective technical safeguards. Large volumes of data can attract interest from outside parties and thus require more effective safeguards. Personal data must be secured at all stages of processing, that is, from collection to erasure.

Data must be protected from access by third parties. 'Third parties' means everyone without a basis or right to process the personal data.

In electronic systems, third-party access to personal data can be prevented with access rights management. The controller must ensure that only persons whose duties give them the right to process personal data can gain access to the data. Remember that viewing the data also counts as processing. When a person changes roles within the club, you should also remember to immediately deactivate their access rights to systems they are no longer entitled to access.



Example

In a sports club, the coaches and team manager of a football team have the right to process the personal data of their team's players but not the personal data of players from other teams in the club.

You should use individual usernames in your systems. The use of shared usernames is not recommended. With individual usernames, the controller can control and verify the processors of personal data, including retrospectively.

The controller must check the default settings of new systems and applications before starting to use them. With regard to data protection, you should check that all users cannot see personal data by default.



Remember

Check the default settings of new systems and applications to ensure that they are not collecting unnecessary data or allowing too many users to see personal data.



What does data security mean?

Data security is one way of implementing data protection. It is intended to protect data and information systems. Among other things, it refers to organisational and technical measures taken to ensure the confidentiality and integrity of data, usability of systems and the realisation of the rights of the data subject.

Who has the right to process personal data?

The controller must specify the persons who have appropriate grounds for processing personal data in any given situation. You should also document these grounds. Appropriate grounds can include both regular work duties and one-off circumstances.

8. Define storage periods for personal data and erase unnecessary data

Limiting the storage of personal data is one of the principles of data protection. The erasure of personal data must also be taken into account in hobby activities so that personal data is not being stored unnecessarily. As a general rule, personal data may only be stored for as long as necessary.

The controller must determine how long each type of personal data must be stored and define a process for the erasure of data. If the controller does not see to the erasure of unnecessary personal data, there is a risk that data will be stored for years without a legal basis for processing. If this is the case, more personal data can also be disclosed to outsiders in the event of, for example, a data leak, than if the personal data had been appropriately erased when no longer necessary.

The format in which personal data is being processed must be taken into consideration in their storage and erasure. Participants must be informed of the storage period of personal data, or at least of the criteria used to determine the storage period. Determining storage periods and planning storage are part of the controller's obligation to demonstrate compliance with data protection regulations.

8.1. Storage period

The storage periods of some types of personal data, such as data related to employment or accounting, have been laid down by law. When this is the case, the data is stored for the statutory period and then erased.

Specific storage periods have not been provided for all types of personal data, however. In such cases, the controller must determine how long each type of personal data will be stored. The rule of thumb for determining the storage period is to only store personal data for as long as necessary for the purpose for which it was collected. Data must be erased when there are no grounds for processing them any more and they are not need for the organisation of hobby activities.

The sensitive nature of the data and the potential risks caused to the participants by its disclosure must be taken into account in the storage of special categories of personal data. In particular this must be taken into account when it comes to children's health information. Health data must be stored so that outsiders cannot access it and may not be disclosed to people who do not need it.

A good way for controllers to define the storage period for personal data is to review all types of personal data being processed and examine the purpose of processing each type in each connection. The controller can then define storage periods for each item or type of personal data based on their purpose. When determining storage periods, the hobby organiser must also take into account different scenarios, such as when someone quits the hobby. Some data can be erased immediately when the participant quits.



Example

A sports club is organising a kick-off event for the autumn season at its home arena. The club asks participants to register for the event so that it can get the right number of water bottles with the club logo as gifts for the participants.

Since it is the controller of the data, the club defines the storage period for the registration data. Because the purpose of processing the registration data is ensuring that enough water bottles are acquired, the data can be erased immediately when no longer needed, that is, when the water bottles have been ordered.

8.2. Storage location

Personal data is stored in electronic format in various systems, such as enterprise resource management systems, and in applications and electronic documents. When data is stored in electronic format, the controller must ensure that it can only be accessed by people who have the right to process the data, for example in their work tasks.

Personal data kept on paper must be stored out of reach from people who are not authorised to process them. You can store papers in a locked cabinet that only authorised people can access.

Also take changes in staff must into consideration in the storage of personal data, so that people who are no longer involved in the club's activities cannot process data without an appropriate basis.

8.3. Erasure

Personal data must be erased at the end of its storage period. Different types of data can be erased in different ways and at different times, depending on their storage periods.

The data can be erased automatically or manually, depending on its form and place of storage. Ensure that personal data is erased from everywhere it has been processed and stored. For example, also delete personal data kept in cloud storage from downloaded files and emails. Do not forget to erase backups as well.

Personal data stored on paper must be destroyed appropriately, so that no unnecessary personal data is left forgotten in binders or at the back of filing cabinets. Paper documents can be destroyed by shredding or deposited in a confidential waste bin, for example.



Example

An athletics club is holding a Christmas party for all of its athletes. The club requests information on the participants' special diets and allergies with the LEAP electronic survey form. After the party, the club destroys all data on the participants' special diets, because the data was only collected for the Christmas party meal and will not be needed after that. The club ensures that no personal data collected with the LEAP survey form remains in the LEAP service, in other information systems used by the club, or on paper.



What do you need to do when a child quits the hobby?

Data must be erased when it is no longer necessary for the purpose for which it was collected. For example, the hobby organiser can have a designated contact person for quitting notices who erases the club member's data in the agreed manner.

What do you need to do when someone involved in the club's activities, e.g. a coach or team manager, quits their role?

The coach or team manager must make sure that they do not have any personal data related to the hobby activity in their possession when they quit. They must erase all personal data related to the hobby, for example from their email, and destroy any papers containing personal data. The hobby organiser should change the passwords of social media accounts to which the person had access and agree to whom the data in the leaving person's possession will be transferred.

The controller is responsible for ensuring that personal data is not processed for longer than is necessary and for instructing those processing data in the hobby activity on the appropriate erasure of the data. When drawing up such instructions, the hobby organiser should remember that the roles of people involved in hobby activities can change at short notice. It is also important to provide orientation training to newcomers to the activity, such as new coaches, team managers, treasurers, volunteers and custodians.



Remember

Minimise the storage of personal data: erase data immediately when it is no longer necessary. Also remember to delete backups.



Example

A Finnish baseball club provides team-specific email addresses to its team managers for conducting the team's business. When the team manager changes, the previous team manager's access to the email account can be revoked and the new team manager can be given access to it. This way, the team managers do not have to use their personal email accounts for team matters and email messages related to the team manager's duties are available to the new team manager. The baseball club has instructed team managers to only use the email address for conducting the team's business.

9. Demonstrate compliance with data protection legislation

A controller must be able to demonstrate that it complies with data protection legislation. This is called 'accountability'. Accountability also means that certain measures must be written down, or documented.

The controller must take all measures required by accountability. Such technical and organisational measures include the provision of training, instructions and orders to personnel, building surveillance, supervision of personal data processing, information system security, data encryption, technical limitations, as well as audit and surveillance systems.

The extent of accountability depends on factors such as the size of the organisation and the volume and types of personal data processed by the controller. The controller must ensure accountability already at the planning stage of processing.

The purpose of accountability is to demonstrate how the controller respects the privacy of the people whose data it is processing. Accountability increases trust in the controller.



Remember

Document your data protection processes so that you can demonstrate your compliance with data protection legislation.

The adequacy of documentation and measures must be assessed on a regular basis, for example in connection with Board meetings.

What obligations does a hobby organiser have in the processing of personal data?

1. Fulfil the participants' data protection rights



DATA SUBJECT



CONTROLLER

'Data protection rights' mean the rights related to processing that the data subject has in respect of the controller processing their personal data. When a hobby organiser processes personal data as a controller, it must ensure that the data subjects' data protection rights are fulfilled. Data protection rights include the participant's right to access their data and to have inaccurate data rectified. The hobby organiser must make it easy for participants to exercise their data protection rights and tell the participants how they can do so.

Data subjects have the following data protection rights:

a. Right to obtain transparent information on the processing of their personal data



Example

A swimming club informs its members of the processing of their personal data in a privacy statement on the club's website.

The data subjects must be informed of the processing carried out by the hobby organiser, and this information must be provided in clear and intelligible form.

b. Right of access to one's data

Data subjects have the right to receive confirmation from the controller whether it is processing personal data concerning them. If the data subject's personal data is being processed, the controller is required to supply a copy of the processed personal data to the data subject.

c. Right to the rectification of data

Data subjects have the right to demand that the controller rectify inaccurate personal data concerning them. Data subjects also have the right to have incomplete personal data completed.

d. Right to the erasure of data and to be forgotten

In certain situations, the data subject has the right to have the controller erase the data concerning them without delay. In some circumstances, participants have the right to have their data erased. However, the hobby organiser may sometimes have the right to keep or publish the data even though the member has demanded that they be erased. The hobby organiser may be required to keep the data for a certain period to comply with the law, for example.

e. Right to the restriction of processing

A data subject can request the controller to restrict the processing of personal data concerning the data subject. This means that, apart from storage, the personal data subject to the restriction may only be processed with the data subject's consent, in connection with a legal claim, to safeguard the rights of another person, or for an important public interest.

f. Right to data portability

A data subject has the right to receive the personal data which they have provided to a controller in a structured, commonly used and machine-readable format, as well as the right to transmit that data to another controller should they wish. The data subject has the right to have the data transmitted directly from one controller to another, where technically feasible.

g. Right to object to the data processing

In certain situations, the data subject has the right to object to the processing of their personal data, that is, request the controller not to process it at all. If the data is being processed in the public interest, in the exercise of public authority vested in the controller, or for pursuing the legitimate interests of the controller or a third party, the data subject can object to the processing on grounds relating to their particular situation.

h. The right not to be subject to a decision based solely on automated processing

The data subject has the right to demand that decisions concerning them are made by a human.



What do you need to take into account when a data subject wants to exercise their data protection rights?

As a rule, the controller is required to respond to the request within one month of receiving the request. The response must describe the measures taken by the controller due to the request.

If there are many requests or they are complex, the controller can notify the data subject that it needs more time to process them. In such cases, the deadline can be extended **by at most two months**. The controller must notify the data subject of the extension within **one month** of receiving the request.

What do you need to take into account if the controller refuses the request?

If the controller refuses the data subject's request, it must justify the refusal and notify the data subject of it within **one month** of receiving the request. The controller must have a legal basis for its refusal.

The controller must also inform the data subject of their opportunity to lodge a complaint with the Office of the Data Protection Ombudsman and of the data subject's other legal remedies.

The contact details of the hobby organiser or person responsible for fulfilling the rights of the data subject must be easy to find. You do not need to give the name of a specific individual in the contact details. For example, you can provide just an email address (e.g. dataprotection@sportsclub.eg) that the person responsible for data subjects' requests has access to.

The extent of the rights of the data subject depends on the basis of the processing. If the basis is the controller's legal obligation, the public interest or the exercise of public authority, the rights of the data subject are more limited than in processing based on agreement, consent or the controller's legitimate interest.

The rights of the data subject do not always apply to all personal data. For this reason, it is important to consider how the rights and requests of data subjects will be fulfilled in practice.



Remember

Design a process for fulfilling the rights of the data subjects: how can the data subjects contact you to exercise their rights, who replies to their requests, how is the data subject identified, and how are the requests fulfilled in practice. Also remember to document the requests. Take the fulfilment of data protection rights into account also when procuring new systems.

If a hobby organiser processes the personal data of a child or adolescent, it must take into account that the minor's custodian may also have the right to exercise the minor's data protection rights on their behalf. On the other hand, minors also have the right to their own data, and it may not be permitted to disclose their data to their custodians in every case.

2. Describe the hobby organiser's processing of personal data with a record of processing activities

A record of processing activities is a written description of the personal data processing carried out by the organisation. Drawing up a record of processing activities makes the hobby organiser's data protection work more systematic and helps with the documentation of processing. The record of processing activities is intended for the organisation's internal use.

A record of processing activities must be drawn up if

- the organisation has over 250 employees; or
- the processing of personal data is not occasional;
- the processing is likely to result in a risk to the rights and freedoms of the data subject; or
- the processing includes special categories of personal data.

Hobby activities often involve the regular processing of at least participants' and club employees' personal data. If this is the case, such processing activities must be included in the record.

The record serves as a tool for conceptualising the processing of personal data. It can also be used to demonstrate that personal data is being processed according to data protection legislation. The record of processing activities is a separate document from the privacy statement, which is used to inform data subjects. The record is not intended for informing the data subjects directly, but can be helpful in producing information intended for data subjects.

The Office of the Data Protection Ombudsman has drawn up a template for the record. The template is available on the Office of the Data Protection Ombudsman's website.

Read more: [Record of processing activities | Office of the Data Protection Ombudsman](#)³



Remember

Draw up a record of processing activities for the personal data processing required by the hobby activities.

³ <https://tietosuoja.fi/en/record-of-processing-activities>



What information must be included in the record of processing activities?

The record must include the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- 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 or international organisations;
- transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) of the GDPR, the documentation of suitable safeguards;
- the envisaged time limits for erasure of the different categories of data or the criteria for determining such time limits; and
- a general description of the technical and organisational security measures, such as the encryption of personal data, the ability to ensure the confidentiality, availability and resilience of information systems, as well as processes for regularly evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3. Agree on processing

If the hobby organiser uses a third party for the processing of personal data, the organiser must ensure that a written processing agreement is signed with them. Making an agreement ensures that the controller's obligations will be fulfilled also when the personal data is being processed by a third-party processor on behalf of the hobby organiser.

Before drawing up the agreement, you should define the roles related to the processing: who is the controller and who the processor processing data on behalf of the controller. For example, a payroll clerk who calculates and pays the wages of club employees can be a processor. In this situation, the hobby organiser is the controller, since it determines who receives wages and on what grounds.

The controller can only outsource the processing of personal data to processors that have adequate safeguards in place for ensuring data security.



Example

A judo club uses a third-party IT provider's ERP system for processing club members' personal data. The IT provider is the processor of the personal data being processed in the system, while the judo club is the controller. The club makes a written agreement with the IT provider on the processing of personal data in the ERP system so that it can make sure that the IT provider follows the club's data protection policies and fulfils its obligations related to the processing.

In the agreement, the controller and processor agree on how the processor must process and secure the personal data. The agreement must specify the object and duration of the processing, nature and purpose of the processing, type of personal data and groups of data subjects, as well as the controller's obligations and rights. The processor must also ensure that its employees with access to the personal data only process it according to the controller's instructions.



Remember

Draw up processing agreements with third-party processors who are processing personal data on the hobby organiser's behalf.

4. Assess the risks and impact of processing

The hobby organiser must always assess the risks related to the processing of personal data before starting processing. If the processing is likely to involve a high risk to the data subjects, a data protection impact assessment is required. The data protection impact assessment is designed to identify, assess and manage risks related to the processing of personal data.

The impact assessment concerns risks caused by the processing of personal data and the measures required to address those risks. An impact assessment must be made when the planned processing is likely to cause a high risk to the rights and freedoms of individuals. It is intended to be a continuous process of identifying and managing risks. The impact assessment must be made before the start of processing and updated whenever necessary.



What does 'risk' mean?

In the GDPR, 'risk' means physical, material or non-material damage potentially caused to the data subject by the processing, in particular where the processing may give rise to discrimination, identity theft or fraud, financial loss, social disadvantage or the reversal of pseudonymisation.

The necessary safeguards must be in proportion to the risk caused by the processing: the higher the risk, the more effective safeguards are needed. Processing special categories of personal data, children's data, or a large volume of personal data concerning a large group of people can cause a high risk.

The level of risk is assessed on the basis of the nature, scope, frequency, context and purposes of the processing. The more extensive and regular the processing and the more sensitive the personal data, the higher the potential risk to data subjects. If an association is processing sensitive data or special categories of personal data on a large scale, it must conduct a data protection impact assessment of the processing. For example, processing the health data of club members may require an impact assessment.



When do you need to conduct a data protection impact assessment?

A data protection impact assessment must be made when the planned processing can cause a high risk to the rights and freedoms of people. Examples of high-risk processing requiring an impact assessment include the use of new technologies for the processing, processing special categories of personal data on a large scale, and processing the personal data of people in a vulnerable position (e.g. children, employees and older persons).



Remember

Identify and assess the risks caused to data subjects by the processing of personal data. Conduct a data protection impact assessment if the risk is high.

The Office of the Data Protection Ombudsman has drawn up instructions to support controllers in conducting data protection impact assessments, along with a simple Excel tool that can be used for the impact assessment.

Read more: [Impact assessment | The Office of the Data Protection Ombudsman](#).⁴

⁴<https://tietosuoja.fi/en/impact-assessments>

5. Report personal data breaches



Given enough time, practically everyone who processes personal data experiences a personal data breach. Therefore, it is important for hobby organisers to define a process for handling personal data breaches. It must ensure that everyone taking part in the processing is able to identify personal data breaches and take the agreed-upon action. In certain cases, the Office of the Data Protection Ombudsman and the victims of the personal data breach must be informed of the breach.

A personal data breach can result in, for example, identity theft or fraud, reputation damage or the disclosure of confidential personal data.



What is a personal data breach?

A personal data breach means an incident that results in the destruction, loss, alteration or unauthorised disclosure of personal data, or that grants a party not authorised to process the data access to personal data. Examples of personal data breaches include

- the loss of a data transfer medium, such as a USB memory stick;
- the theft of a computer;
- hacking or a cyber attack;
- malware infection;
- mailing an invoice to the wrong person; or
- unauthorised access to personal data.

A personal data breach can result in, for example, identity theft or fraud, reputation damage or the disclosure of confidential personal data.

The most important thing is to initiate damage control measures as soon as possible after the personal data breach has been detected. The hobby organiser should draw up a process for handling personal data breaches and designate a person (such as a Data Protection Officer) responsible for investigating and documenting breaches.



When does a personal data breach have to be reported to the supervisory authority?

If the personal data breach causes a risk to the data subjects, it must be reported to the Office of the Data Protection Ombudsman within 72 hours of discovery. The report can be made using the notification form on the Office of the Data Protection Ombudsman's website.

When do the victims of a personal data breach need to be informed of the breach?

If a personal data breach causes a **high risk** to the data subjects, the people affected by the breach must also be informed of it so that they can take the necessary precautions and prepare for the risks caused by the personal data breach.

In certain exceptional circumstances, the controller is not required to notify the data subjects of a personal data breach:

- the controller has implemented appropriate technical and organisational protection measures and they have been applied to the personal data affected by the personal data breach (in particular those that render the personal data unintelligible to outsiders, such as encryption);
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; or
- it would involve disproportionate effort, for example because the controller does not know who the data subjects are.

If the data subjects cannot be contacted personally, a public communication or similar measure whereby the data subjects are informed in an equally effective manner must be used.

If the controller has not communicated the personal data breach to the data subject, the supervisory authority may require it to do so.

The controller is obliged to document all personal data breaches, their effects, and the corrective measures taken. This means that, if a personal data breach occurs, you should keep all emails and other correspondence related to the matter, save system log data for the duration of the incident, and write down all measures taken and all individuals who have participated in managing the incident. The controller is responsible for evaluating the consequences of the personal data breach and whether the supervisory authority and data subjects should be notified of it.

Read more: [Personal data breaches | The Office of the Data Protection Ombudsman](#) ⁵



Remember

Detect personal data breaches, assess the risks they cause to the data subjects, and notify the supervisory authority and people affected if necessary. Document the events and the steps of managing the breach.



Example

The tennis coaches have their monthly meeting in the tennis hall's cafeteria. There was no one else in the cafeteria during the meeting, but one of the coaches forgot a paper containing players' health information on the table after the meeting. A group of players sitting in the cafeteria after their game found the paper and gave it to a cafeteria worker. The cafeteria worker told the tennis club's president about what had happened.

The tennis club assessed the matter and decided that the incident could cause a high risk to the data subjects, that is the players, because the paper left on the table contained their health information and the tennis club did not know how many people could have seen the paper. The tennis club reported the personal data breach to the Office of the Data Protection Ombudsman and the people whose information was on the paper.

⁵<https://tietosuoja.fi/en/personal-data-breaches>



What information do you need to give to the supervisory authority about a personal data breach?

The data breach notification filed with the supervisory authority must include at least the following information:

1. a description of the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the name and contact details of the data protection officer or other contact point where more information can be obtained;
3. a description of the likely consequences of the personal data breach; and
4. a description of the measures taken by the controller to address the incident, including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible to provide the above-mentioned information at the same time, the information may be provided in phases without undue further delay.

What information do you need to give to the data subjects about a personal data breach?

Individuals affected by the breach must be provided the following information about the incident in clear and plain language:

1. what has happened;
2. what the likely consequences of the personal data breach are to the person;
3. what measures the controller has taken to address the personal data breach and what measures it has taken to mitigate the possible adverse effects of the breach; and
4. the contact details of the data protection officer or other contact point where more information can be obtained.

6. Only transfer personal data out of the EU if the conditions are met

The level of data protection may not meet the EU's requirements when personal data is transferred out of the EU and European Economic Area (EEA). That is why there are certain conditions to be met if you intend to transfer data out of the EEA.

The hobby organiser must identify whether its activities involve the transfer of data to third countries (countries outside the EU or EEA). Personal data can be transferred via various systems and electronic services, for example.

In addition to the EU Member States, the EEA comprises Iceland, Liechtenstein and Norway. Personal data may be transferred to these countries on the same grounds as within Finland. Transferring personal data outside these countries can cause risks to the persons whose data is being transferred.

For the transfer of personal data to be permitted, both of the conditions below have to be met:

1. the processing of personal data must be allowed in the circumstances in question; and
2. there is a basis listed in the GDPR for the transfer. In addition, you need to assess on a case-by-case basis whether supplementary safeguards are needed to ensure an adequate level of data protection.

The use of each basis for transfer is subject to certain conditions. The hobby organiser must assess which of the bases for transfer is appropriate. If the conditions of none of the bases for transfer are met, the personal data may not be transferred.



Remember

Make sure that transfers of personal data out of the EEA comply with the requirements set for them.



What does the hobby organiser need to take into account when transferring data out of the EEA?

1. The hobby organiser must first determine whether it or its processors or subprocessors are transferring personal data out of the EEA.
2. If personal data is being transferred out of the EEA, the hobby organiser must ensure that the processing is permitted in those circumstances and that a specific basis for transfer has been specified for the transfer of the personal data.
3. The controller must then check whether the third country's legislation and/or practices guarantee a level of protection corresponding to EU requirements for the personal data being transferred.
4. If the chosen basis for transfer does not in itself guarantee an adequate level of data protection, it can be supplemented with various safeguards in certain situations. The hobby organiser must then determine whether such safeguards can be adopted.
5. You should document your assessments of international transfers of personal data.

Read more: [Transfers of personal data out of the European Economic Area | Office of the Data Protection Ombudsman](#).⁶

⁶<https://tietosuoja.fi/en/transfers-of-personal-data-out-of-the-eea>

7. Give people involved in the hobby instructions and training in data protection

Everyone involved in hobby activities deals with data protection in a variety of everyday situations. Everyone involved in hobby activities has responsibilities related to data protection. The hobby organiser's level of data protection is only as good as the level maintained by the people involved in the hobby. Data protection is a permanent part of the daily work of organising a hobby, not a one-off exercise or something that can be taken care of with a couple of documents.

People with access to personal data must process it according to the controller's instructions. For everyone involved in the processing of personal data to be able to correctly implement data protection in the hobby, the hobby organiser must ensure their competence by drawing up instructions for the processing of personal data and/or by arranging for their participation in data protection training. It is also important to give new personnel an orientation to data protection.

For the practical implementation of data protection, the club or association can draw up data protection instructions of various levels or checklists for different roles. The important thing is to emphasise the need to be careful when processing personal data and to instruct people to only process personal data for purposes related to the hobby.

You should give people guidance on confidentiality, for example, so that those involved in the hobby will not disclose information to third parties unlawfully. The non-disclosure obligation continues even after a person quits the hobby. The controller should define what 'third-party' means in this context.



Example

As a rule, the personal data of players in hockey team A may not be disclosed to the team manager of hockey team B if the team manager is not involved in the activities of hockey team A in any capacity.

Those involved in the hobby should be aware of the roles in which they are processing personal data in any given situation. If a person has several roles, they must know how they are permitted to process personal data in each role.



Remember

Instruct people involved in the hobby on the processing of personal data if their role involves processing.

The GDPR4CHLDRN-project by the Office of the Data Protection Ombudsman and TIEKE has developed quizzes of data protection skills for those in an administrative role in associations and for coaches and instructors. The quizzes can be used to assess basic understanding of data protection. By scoring high enough on the quiz, the participant will receive a visual badge in a report to represent their data protection skills. The quizzes can be used to support the induction of new staff in associations. Those who are already involved in the association can be asked to take the quiz for example every year, and to refer to the additional material indicated in the report after the quiz.

View the quizzes: [Quizzes | Data protection in hobbies](#).⁷

⁷<https://tietosuojaharrastuksissa.fi/en/material-bank/quizzes/>

8. Manage the life cycle of personal data from planning to collection, storage and erasure

The life cycle of personal data processing begins with the planning of processing and ends with the erasure or archiving of the data. Data protection must be taken into account in every stage of the life cycle.

When **planning** the processing of personal data, first determine the legal basis and purpose for the processing. At the same time, consider the principles of personal data processing, informing the data subject and fulfilling their rights, and measures to secure personal data. Conduct a risk assessment and draw up data protection documentation, such as a record of processing activities and a processing agreement. Also define the roles and responsibilities related to processing.

When **collecting** personal data, take data minimisation and accuracy into account. When **using** personal data, remember at least the principle of purpose limitation, access rights management, and the requirements related to the disclosure of data.

When **storing** personal data, you need to pay attention to the storage location and the necessary technical safeguards. When the storage period of personal data expires, the personal data must be **erased** securely and in accordance with the storage periods.

In hobby activities, it can be useful to define processes for at least the following situations related to processing:

- fulfilling the rights of the data subjects;
- detecting personal data breaches and notifying the supervisory authority and data subjects of them;
- data protection impact assessments and agreeing on processing in connection with new acquisitions;
- the collection of personal data: what data is collected and by whom, where it is stored, and when and how it is erased; and
- the erasure of personal data when someone quits the hobby: what do the various parties (coach/instructor, team manager, club employee) need to take into account.



Example

A gymnastics club has defined a process for erasing personal data when a gymnast quits. When a gymnast tells their coach that they are quitting the hobby, the coach notifies the club's director of coaching and the team manager of it. The team manager then notifies the team's treasurer. The director of coaching lets the club secretary know.

The coach, team manager and treasurer erase the necessary data concerning the gymnast according to the club's instructions, for example from their email and paper documents. The club's director of coaching and secretary erase the required data from the club's ERP system and notify the national association that the gymnast has left the club. The gymnastics club will have to keep some data for the statutory period and cannot erase it right away.



Brief data protection checklist for the Boards of hobby organisers

1. Identify the hobby organiser's own role in the processing of personal data in various contexts.
2. Identify the personal data being processed in the hobby activities, the persons processing it, and the roles of each party in the processing.
3. Define a purpose for the processing of personal data and only process the data for that purpose. If you change the purpose, the data subjects must be notified of it before the start of processing.
4. Specify the bases for processing personal data for the various purposes.
5. Minimise the processing of personal data in connection with the hobby activities. If you have to process personal data, think carefully about which personal data are necessary for which purpose.
6. Check the accuracy of participants' personal data regularly and rectify inaccurate data everywhere it is being stored. Ask participants to notify you of any changes to their data.
7. Inform the various parties (e.g. the participants, employees, instructors, coaches, custodians and stakeholders) of the processing of their personal data. Pay special attention to the intelligibility of information provided to children.
8. Minimise the storage of personal data: erase data immediately when it is no longer necessary. Also delete any backups.
9. Design a process for fulfilling the rights of the data subjects: how can the data subjects contact you, who replies to their requests, how is the data subject identified, and how are their data protection rights fulfilled in practice.
10. Detect personal data breaches, assess the risks they cause to the data subjects, and notify the supervisory authority and people affected if necessary. Document the events and the steps of managing the breach.
11. Draw up a record of processing activities for the hobby.
12. Draw up processing agreements with third-party processors who are processing personal data on the hobby organiser's behalf.
13. Identify and assess the risks caused to data subjects by the processing. Conduct a data protection impact assessment if the risk is high.
14. Instruct people involved in the hobby on the processing of personal data.

What should you take into account when publishing photos and videos?

Children are sometimes photographed or videoed in their hobbies. A photograph or video constitutes personal data if people can be identified from them.

You need a legal basis for processing and publishing photos of participants. For example, the hobby organiser can ask for the child's or their custodian's consent for publishing the photos. If you request the consent from the child themselves, you need to consider the child's age and ability to assess the significance of their consent. Read more about requesting consent from minors in the section "Consent from minors" on page 20.

It is the hobby organiser's responsibility to demonstrate that consent has been given. For this reason, you should request the consent in writing.

To publish a photograph, you need the consent of every identifiable person in it. If you have not obtained everyone's consent, you cannot publish the photo in a form that enables the identification of people who have not given their consent for the publication.

People also have the right to withdraw their consent for the publication of photographs. If someone withdraws their consent, you normally have to remove the photo or edit it to render the person unidentifiable.

Consent for taking and publishing photographs and video must be freely given. That means that it must be requested in a manner and context that let the participant refuse their consent without fear of consequences such as falling into disfavour. You should be especially mindful of this when requesting consent directly from a child.

When publishing photos and video on social media, for example, you should remember that the social media platform may use the photos and video for its own purposes. The people identifiable from photos must be informed of where the photos will be published and of the possible consequences of such publication (for example, the possibility of the photos spreading or being used for other purposes).

You should draw up instructions for taking and publishing photos and video for everyone involved in the hobby.



When can a hobby organiser publish photos and video featuring children, e.g. on its website?

The hobby organiser needs a legal basis for publishing photos and video of people in the hobby. For example, the hobby organiser has to ask for the child's or their custodian's consent for publishing photos and video. The consent must be specific, which means that it must be explicitly stated that photos of the child will be published on the hobby organiser's website.

The hobby organiser must have a legal basis for publishing the personal data of participants and processing it, also on social media. It is also a good idea to draw up instructions for the use of social media.

What should you take into account when processing health data in hobby activities?



SENSITIVE
DATA

Information on a child's allergies, illnesses or medication is often essential for guaranteeing the child's health and safety in hobbies and leisure activities.

Health data is a special category of personal data, the processing of which is generally prohibited. The processing of health information can be permitted, for example based on the data subject's consent. If health data is collected based on the consent of the child or their representative, they must only be requested to provide health data necessary for the child's health and safety.

Data may not be collected just in case or for possible future needs. For example, it is not permitted to collect data on food allergies if there is no appropriate basis and need for it at the time. The hobby organiser must be able to demonstrate that the child or their representative has given their explicit consent for processing the child's health data.

Read more about requesting a consent in the section "Consent requires an indication of the participant's wishes" on page 19 and in the section "Consent from minors" on page 20.



Example

The coach of a Finnish baseball team sends the parents of children who join the team a link to a form asking for information on the child's illnesses or medication which the coach should be aware of during training to ensure the child's health and safety. The baseball club has instructed coaches to collect the players' health data with the form in question, so that the children's health information will be obtained in the manner specified by the club and only the appropriate coaches who need to process the data can do so.

The child's custodian logs into the form with two-factor authentication. The form asks the custodians to only report illnesses and medication that the coaches need to know about to ensure the child's health and safety during training. The form also asks for consent for the processing of health data and states that the consent can be withdrawn at any time. Since consent for processing the child's health data is being requested with an electronic form, the baseball club will be able to demonstrate that the custodian has given their consent for the processing of the child's health data and that the club has a basis for processing the data in question.

What should you take into account when disclosing personal data in hobby activities?

Circumstances may arise in which you need to disclose personal data to third parties in connection with hobby activities. You must notify the data subjects in advance of the disclosure of personal data and of what data concerning them will be disclosed to third parties.

You always need a legal basis for the disclosure of personal data, as for any other form of processing. If the hobby organiser's right to disclose the data subject's data to third parties has not been provided for by law, the hobby organiser must ask for the data subject's specific consent for the disclosure. In such situations as well, the hobby organiser must inform the data subjects of how their personal data will be used and for what purposes. Data subjects must be informed in advance of the disclosure of data to third parties.

Please remember that the telephone numbers and addresses of some data subjects may be secret. Informing the data subjects of the disclosure of personal data is particularly important in such cases. A person can also have a non-disclosure for personal safety reasons or may be otherwise unwilling to have their data shared with other club members or the hobby organiser's partners.



Can a hobby organiser publish the results of individual club members, e.g. in a competition or skill contest?

Informing the data subjects and the legal basis for publication need to be taken into account when publishing the competition or skill contest results of individuals, e.g. on the hobby organiser's website. It is the controller's responsibility to assess the lawfulness of the publication. In any case, the participants in the competition must be informed that the results will be published.

If the hobby organiser will publish the results itself, it must first consider which legal basis it will use for the publication. In some cases, the publication can be based on the controller's legitimate interest. The data subject then has the right to object to the publication of their personal data. The controller must inform the contestant that their data will be published and that they have the right to object to the processing of their personal data.

The results could also be published based on the data subject's consent, in which case the hobby organiser could ask the contestants for their specific consent to the publication of personal data already when registering for the competition. The data subject can withdraw their consent at any time, upon which the data must be erased.

Clubs and associations must consider on a case-by-case basis whether data can be published based on the controller's legitimate interest or whether the data subject's consent is required.

If the hobby organiser discloses the data subjects' personal data for commercial purposes or for cooperation with commercial partners, it must consider the lawfulness of the processing, especially if it intends to disclose the personal data of children for commercial purposes.

ANNEX 1: CONSENT FORM – TEMPLATE

CONSENT [enter the purpose of the consent here, e.g. for a photograph]

I consent to [specify for what purpose the consent is being requested. If the personal data will be processed for several purposes, you need to request consent separately for each purpose. E.g.

having my photographs taken during football practice

having my photographs published on the football club's website

having my photographs published on the football club's Instagram account]

Giving your consent is voluntary. The data will not be used for automated individual decision-making or profiling [the use of data for automated individual decision-making and profiling must be declared on the consent form. If you will use the data for such purposes, disclose it here.]

I can withdraw my consent at any time by contacting [enter the point of contact for withdrawing consent here, e.g. the team's coach. It must be as easy to withdraw consent as to give it]. After I have withdrawn my consent [enter the data that has been processed based on the consent here, e.g. "my photographs"] will no longer be processed and will be erased [data being processed on the basis of consent must be erased after consent is withdrawn unless there is another legal basis for retaining the data].

The controller of the data processed based on this consent is [enter the controller of the personal data here, e.g. Football Club.] I can find more details [enter the location of the controller's information related to the processing of the personal data here, e.g. "about the processing of my photographs on the football club's website", and add a link to the data protection information].

date

signature

name of dependent

ANNEX 2: COMICS TO INFORM ABOUT DATA PROTECTION














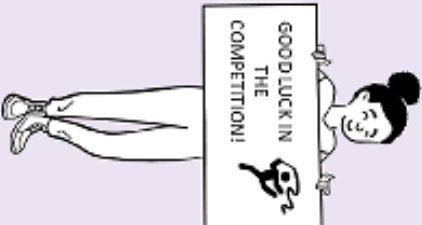
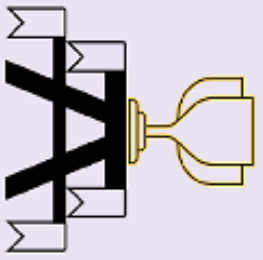
The following comic strips depict situations related to data protection in hobbies and are specifically designed to inform children and young people about the processing of personal data. The comic strips can be used to increase awareness within your association. Feel free to print them and pin them to your walls to remind people about this important topic!

The examples showcased in these comics are fictional and cannot be applied as such. The controller should always assess the information provided to data subjects on a case-by-case basis, taking into account data protection legislation.



<p>Hi coach!</p> <p>Hi! Nice that you could make it to practice.</p> <p>FOOTBALL TEAM 812 youth team</p>	<p>We've been told about data protection at school, and we got an assignment to ask about the processing of our personal data in hobbies.</p> <p>I know that 'personal data' means some kind of information that people can use to identify me, like my name, email address and personal identity code.</p> <p>I have heard that the football club is storing my personal data in the FOOTIE system. Why are they doing that? And what else can you tell me about the subject?</p>	<p>It's really great that you asked! Data protection is important.</p> <p>The football club processes different kinds of personal data so that you can play football. Your personal data is processed so that we coaches will know whether you will come to training and that we can register our team for training camps and tournaments. These are just a few examples.</p> <p>The football club processes your name, telephone number, email address, address and training amounts, as well as the results of your skill tests.</p>
<p>Your personal data is only processed by football club personnel who have the right to do so. We coaches process your personal data for training purposes, and club employee Pekka processes it for maintaining the club's membership register. Our team manager Ossi processes your personal data in connection with signing up for training camps and tournaments, and treasurer Mike does so in connection with various payments.</p> <p>The football club is using the FOOTIE system for processing personal data to monitor training amounts. We coaches have access to our team members' personal data in the FOOTIE system.</p> <p>Personal data is stored in the FOOTIE system for two years, after which it is automatically erased.</p>	<p>You have the right...</p> <ul style="list-style-type: none"> to obtain information on the processing of your personal data; to access your own data; to rectification of your data; to the erasure of your data and to be forgotten; to restrict the processing of your data; to data portability; to object to the processing of your data; and not to be subject to a decision based solely on automatic processing. <p>Not all rights apply in all situations, but you can still me for more details if you like.</p>	<p>Thanks for telling me! Now I know a lot more about the processing of my personal data.</p> <p>I'm going to change into my football boots now, see you on the pitch!</p>

This example is about an imaginary case and cannot be applied as it is. The controller must always assess the need to inform the data subjects on a case-by-case basis, taking the data protection legislation into consideration.

 <p>Welcome to the Finnish championships in aesthetic group gymnastics! Fantastic to have you.</p> <p>The gymnast gymnastics club processes your personal data in connection with entering competitions to ensure that you can participate and that the competitions proceed smoothly.</p> <p>In this document, I will describe the processing of personal data by the gymnast gymnastics club so that you will know how your personal data is being processed.</p>	 <p>The results will be published on the gymnastics club's website by division. The names of individual gymnasts will not be published. The results will be listed by team. The personal data will be processed within the EUEEA.</p> <p>Personal data collected in connection with signing up for competitions will be used two weeks after the competition.</p> <p>The results of the competition will be erased from the gymnastics club's website in two years from the end of the competition.</p>
 <p>For the processing of personal data in the Finnish championships at hand, the controller is the competition organizer:</p> <p>Gymnast gymnastics club Gymnast avenue 1, Gymnast Town data.protection@gymnastgymnasticsclub.fi</p> <p>By law, a basis must always be specified for the processing of personal data. In the Finnish championships, the gymnast gymnastics club processes personal data based on its legitimate interest. Your allergy information is processed with your explicit consent.</p>	 <p>You have the right...</p> <ul style="list-style-type: none">  to obtain information on the processing of your personal data;  to access your own data;  to rectification of your data;  to the erasure of their data and to be forgotten;  to restrict the processing of their data;  to object to the processing of their data; and  not to be subject to a decision based solely on automated processing. <p>You can exercise your rights by contacting our club's data protection contact person at data.protection@gymnastgymnasticsclub.fi.</p>
<p>To organize the competition, the gymnast gymnastics club processes the following personal data concerning you:</p> <ul style="list-style-type: none">  your name  your birth year <p>Information on your allergies for meals during your registration for the competition.</p> <p>Your personal data was collected in connection with your team's registration for the competition.</p> <p>The personal data is processed by the employees of the gymnast gymnastics club, as well as volunteers taking part in or assisting competitions. The personal data is processed in the gymnast system, with the system supplier acting as the processor.</p>	 <p>GOOD LUCK IN THE COMPETITION!</p> 

This example is about an imaginary case and cannot be applied as it is. The controller must always assess the need to inform the data subjects on a case-by-case basis, taking the data protection legislation into consideration.



Panel 1:

Hi coach!
My telephone number has changed. Do I need to do something about it?

Panel 2:

Hi! Yes! It's good that you told me. You have the right to have your personal data corrected. It's important that we have your correct telephone number so that we can contact you.

I will let the club secretary know after practice. They will change your telephone number in the club's membership register. I will also tell our team manager so that they can change your phone number in our team's details. That will take care of it.

Panel 3:

Wow, that was easy. Thanks coach!

This example is about an imaginary case and cannot be applied as it is. The controller must always assess the need to inform the data subjects on a case-by-case basis, taking the data protection legislation into consideration.