HÖGSKOLAN DALARNA

REGEL

Gäller från och med
2018-08-22

Beslutat av
Rektor

Diarienummer
C 2021/822

Regler för behandling av personuppgifter

Rules for the Processing of Personal Data

Bakgrund

Behandling av personuppgifter regleras från och med 25 maj 2018 av den europeiska dataskydds-förordningen, som då ersätter den svenska personuppgiftslagen. Det innebär förändrade krav vid behandling av personuppgifter. I detta styrdokument fastställs de grundläggande principer som framöver ska gälla för Högskolan Dalarnas behandling av personuppgifter, samt hur ansvaret fördelas.

Datainspektionen[1] beskriver personuppgifter enligt följande: ”*Personuppgifter är all slags information som kan knytas till en fysisk person som är i livet. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter. Ja, till och med ljudinspelningar som lagras elektroniskt kan vara personuppgifter även om det inte nämns några namn i inspelningen. Ett bolagsnummer är ofta inte en personuppgift men är det om det handlar om en enskild närings-verksamhet. Registreringsnumret på en bil kan vara en personuppgift om det går att knyta till en fysisk person medan registreringsnumret på en firmabil som används av flera, kanske inte är en personuppgift*”.

Grundläggande principer

Laglighet, korrekthet och öppenhet

Personuppgifter ska bara behandlas om det är nödvändigt och det finns en rättslig grund för behandlingen. De behandlade uppgifterna ska vara korrekta och hållas uppdaterade. På ett lättillgängligt och med ett klart samt tydligt språk, skall de registrerade informeras hur deras personuppgifter behandlas.

Ändamålsbegränsning

Personuppgifter ska bara behandlas för särskilda, uttryckligt angivna och berättigade ändamål, och får inte senare behandlas på ett sätt som är oförenligt med dessa. T.ex. får uppgifterna även behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Uppgiftsminimering

Insamlade personuppgifter ska vara adekvata, relevanta och nödvändiga för de ändamål för vilka de behandlas.

Lagringsminimering

[1] Hämtat från Datainspektionen 2018-05-21, www.datainspektionen.se/Documents/enkel-kurs-dataskydd.pdf

Personuppgifter får inte lagras som personuppgifter längre än vad som krävs för ändamålet. Därefter ska de raderas eller avidentifieras, om inte andra regelverk kräver arkivering. Uppgifter får dock lagras längre tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål.

Integritet och konfidentialitet

Personuppgifter ska skyddas mot obehörig eller otillåten behandling, förlust, förstöring eller skada genom att lämpliga tekniska och organisatoriska åtgärder vidtas. För att säkerställa detta, och för att förhindra otillåten överföring utanför EU/EES, ska högskolans avtalade IT-tjänster användas vid behandling av personuppgifter.

Ansvarsskyldighet

Den som behandlar personuppgifter ska kunna visa att regelverket följs. Det ska bland annat ske med hjälp av uppdaterade riktlinjer, tydlig information till registrerade, anmälan och förteckning av pågående behandlingar av personuppgifter samt dokumentation av olika ställningstaganden, som riskanalyser och eventuella konsekvensbedömningar.

Roller och ansvar

Nedan följer en beskrivning av olika roller och ansvar som finns förknippade med dataskyddsförordningen och Högskolan Dalarna.

Registrerad

Den person vars personuppgifter behandlas.

Personuppgiftsansvarig

Högskolans ledning (styrelse och rektor) är personuppgiftsansvarig och ansvarar för att lämpliga tekniska och organisatoriska åtgärder vidtas vid behandling av personuppgifter på högskolan. Personuppgiftsansvarig ansvarar också för att pågående behandlingar förtecknas i ett register samt att dataskyddsombudet involveras i dataskyddsfrågor och ges förutsättningar att utföra uppdraget.

Personuppgiftsbiträde

Tredje part som behandlar personuppgifter på uppdrag av högskolan. T.ex. en leverantör av en tjänst eller en samarbetspart. Förhållandet ska regleras med ett personuppgiftsbiträdesavtal.

Högskoledirektör

Utser dataskyddsombud på delegation av personuppgiftsansvarig.

Informationsförvaltningsgruppen

Består av kompetenser från IT, arkiv, registratur och verksamhetsutveckling. Samordnar arbetet med dataskyddsfrågor på högskolan.

Dataskyddsombud

Ger information och råd till verksamheten angående tillämpningen av dataskyddsförordningen.

- Bevakar självständigt att personuppgifter behandlas i enlighet med dataskyddsförordningens krav och i enlighet med interna styrdokument.
- Rapporterar till högskolans ledning.
- Prioriterar arbetet baserat på eventuella risker för registrerade.
- Ger på begäran råd och stöd till verksamheten vid risk- och konsekvensbedömningar av personuppgiftsbehandlingar.

- Fungerar som kontaktperson gentemot tillsynsmyndigheten.
- Fungerar som kontaktperson gentemot registrerade.
- Utarbetar förslag till lokala styrdokument rörande behandling av personuppgifter.
- Sammankallar informationsförvaltningsgruppen.

Medarbetare och student

Ansvarar för att följa högskolans instruktioner gällande behandling av personuppgifter och ska anmäla dessa pågående behandlingar till dataskyddsombudet. Detta gäller även studenter när de behandlar personuppgifter som en del av utbildningen.

Rules for the Processing of Personal Data

Background

Since May 25, 2018, processing of personal data has been regulated by the European General Data Protection Regulation (GDPR), which in Sweden replaced the former Swedish Law on Personal Data (Personuppgiftslagen). This resulted in certain changes in the processing of personal data. This policy document presents the basic principles relating to the processing of personal data at Dalarna University and where responsibility lies.

The Swedish Data Protection Authority[2] (Datainspektionen) describes personal data as follows: "*Personal data is any kind of information that can be linked to a living person. This might for example be your name, address and personal identity number. Photos of people are also classified as personal data. In fact, even sound recordings that are stored digitally can constitute personal data even if no names are mentioned in the recording. A corporate identity number is not personal data but may be in the case of a one-person company. A car's registration number may constitute personal data if it can be linked to a natural person."*

Fundamental Principles

Lawfulness, Accuracy and Transparency

Personal data must only be processed when necessary and when there is a lawful basis to do so. Processed data must be correct and must be kept up-to-date. In clear and comprehensible language, those whose data is being processed must be informed about how their personal data is being processed.

Purpose Limitation

Data may be collected only for specific, explicitly stated and legitimate purposes, and may not be processed at a later time in a manner that is not in keeping with this. For example, data can also be processed for the purpose of archiving for general interest, scientific and historic research purposes or statistical purposes.

Data Minimization

The personal data that is processed must be adequate, relevant and necessary in relation to the purpose for which it is being processed.

Storage Minimization

Personal data may only be retained for as long as it is needed for the purpose. After this, the data must be deleted or be made anonymous, so long as another regulation does not require archiving. Data can, however, be stored for a longer time for the purpose of archiving for general interest, scientific and historic research purposes or statistical purposes.

Integrity and Confidentiality

Data must be protected against unpermitted and unauthorized processing, loss and damage by taking adequate technical and organizational measures. To ensure this and to prevent unpermitted transfer to

[2] From the Swedish Data Protection Authority 2018-05-21, https://www.datainspektionen.se/other-lang/inenglish/about-privacy/what-is-actually-meant-by-personal-data/

countries outside the EU/EES, the University's commissioned IT services must be used for the processing of personal data.

Accountability

Anybody processing personal data must be able to demonstrate that the regulation has been followed. This will be done by using updated guidelines, clear information to the person whose data is being processed, application and registration of ongoing processing of personal data and documentation of different position statements, such as risk analyses and any impact assessments.

Roles and Responsibility

What follows here is a description of the different roles and responsibilities that relate to GDPR and Dalarna University.

Registered Person

The person whose personal data is being processed.

University Responsibility

University management (the University Governing Board and the Vice-Chancellor) are responsible for personal data and for ensuring that suitable technical and organizational measures are taken in the processing of personal data at the University. They are also responsible for ensuring that processing that is in process is listed in a register and that the Data Protection Officer (dataskyddsombud) is involved in data protection issues and is given the means to carry out related work.

Data Controller (Personuppgiftsbiträde)

This is a third party that processes personal data upon direction by the University. It may be, for example, a supplier of a service or a collaborative partner. The relationship must be regulated by a personal data controller agreement.

University Director (Högskoledirektör)

The Director of Administration selects a Data Protection Officer as delegated by those responsible at the university for data processing.

Information Management Group

This group comprises representatives from IT, Archives, the Registrar and those who work with university development. It coordinates the work with data protection issues at the University.10

Data Protection Officer

- Provides information and advice to the organization regarding the implementation of GDPR.
- Independently monitors the processing of personal data so that it is in accordance with the requirements of GDPR and internal policy documents.
- Reports to university management.
- Priorities work based on any possible risks for those whose personal data is registered.
- Upon request, provides advice and assistance to the organization in matters related to risk analyses of personal data processing.
- Acts as the contact person for regulatory authorities.
- Acts as the contact person for those whose data is registered.
- Prepares suggestions for local policy documents that concern the processing of personal data.
- Convenes meetings with the Information Management Group.

Employees and Students

Are responsible for following the University’s instructions regarding the processing of personal data and must report matters in progress to the Data Protection Officer. This is also the case for students when they are processing personal data as part of their education