Personal data protection – privacy statement

The Research Council meets obligations related to protection of personal privacy through its compliance with the Norwegian Personal Data Act and the EU's General Data Protection Regulation (GDPR).

This privacy statement describes how the Research Council of Norway processes personal data.

The Chief Executive of the Research Council is the designated data controller for the Research Council's processing of personal data when we are responsible for deciding the purpose of and means for carrying out such data processing alone or together with others, and in other instances when we are legally obligated to act as data controller.

The Research Council is the data processor when processing personal data on behalf of a data controller.

This privacy statement is structured by topic and is updated on an ongoing basis. It was last updated on 15 February 2019.

Why we process personal data

As the national strategic research administrative body under the Ministry of Education and Research we are required to process personal data in order to realise:

- the secondary objectives, requirements, guidelines and principles established by our policies;
- the subsequent routines and tasks set out in our procedures.

Processing of personal data

Processing of personal data takes place when required by activities subject to our statutes, policies and procedures. For example, we process personal data in connection with the following:

- website traffic;
- review of applications for funding;
- dealing with complaints;
- follow-up of funding recipients;
- organisation of courses, seminars or other events;
- meetings;
- processing of employment applications;
- recruitment and follow-up of employees or contractors;
- communication activities;
- processing of requests for access to public documents in accordance with the Freedom of Information Act.

Kinds of personal data that we process

The personal data we collect and process at any given time will vary depending on the type of activity being carried out.

Examples of the types of personal data collected for processing include name, address, telephone number, email address, national identity number, employer, CV, hourly rates, time sheets for work carried out, and personal or professional affiliations in connection with impartiality assessments.

How we process personal data

Personal data are processed in accordance with the policies and procedures in effect at all times. Most relevant in this context are the policy on the protection of personal privacy, the policy on security, the policy on processing of personal data and our procedure on information security.

We keep records of our personal data processing activities. We notify our Data Protection Officer of all such activities before they are initiated.

We take active steps to fulfil our obligations regarding personal privacy and to ensure that you are able to exercise your rights related to personal data.

We do not process any other personal information and the data we do collect are not stored any longer than is dictated by the purpose of the processing or is required by the statutory framework, such as the Act relating to archiving (Arkivlova) and appurtenant regulations.

More information about privacy protection is provided below by topic:

Application processing and project assessment and follow-up

Personal data in connection with application processing, in the assessment and follow-up of projects that have been granted funding, and in monitoring the use of allocated funding in submitted project account reports are stored in the Research Council's eSøknad online application system via the My RCN web portal and in the ACOS Websak archive system.

The specific categories of information that will be stored will vary in relation to the role in question. The information collected consists primarily of name, national identity number, email address, position, place of employment and role in relation to the project. For persons receiving remuneration from the Research Council, e.g. referees and board members, the information necessary for disbursing the remuneration, such as national identity number (alternatively, a D-number when relevant), is stored in the registry. For referees, information linked to previous involvement in application assessment is also recorded.

Employees, referees, and members of the Executive Board, portfolio boards and others receiving remuneration from the Research Council are registered in Agresso, the Research Council's Enterprise Resource Planning (ERP) system. This is necessary in order to carry out contractual payments and mandatory reporting to Norwegian (and, when applicable foreign) authorities.

Personal data related to application review and project follow-up are normally stored and deleted according to the Research Council's archiving procedures, which comply with the relevant statutory framework.

Use of our website

Web usage statistics

The Research Council's webpages register the IP address of users visiting the site. These data are processed in a de-identified format which prevents the data from being linked to individual persons. These data are collected for statistical analysis to develop and improve webpage content. The statistics are used to find out the number of times different pages are viewed, the duration of these visits, which websites users are visiting from and which browsers are being used.

Web analysis and cookies

We use the analytical tools Google Analytics and Hotjar on our main website, www.forskningsradet.no. By closing the cookie banner that appears when visiting a page, the user consents to our use of cookies, and agrees that the guidelines for privacy protection of Google Analytics will apply.

Google Analytics is set up so that IP addresses may only be processed in an anonymised format. The Hotjar analytical tool employs a cookie for tracking traffic on www.forskningsradet.no.

Cookies are small text files downloaded to the visitor's computer when a webpage is downloaded. We use cookies to generate statistics and for web analysis to provide the best possible functionality and user experience on our webpages.

Most web browsers are configured to handle cookies automatically. A browser's settings may have to be changed if the user does not wish to accept cookies. Blocking cookies may limit a website's functionality. For more information about cookies, visit: www.allaboutcookies.org and www.cookiepedia.co.uk.

An overview of the cookies used on our website is presented in the table below:

Name	Description	Duration
_hjIncludedInSample	Hotjar cookie. This session cookie is set to let Hotjar know whether that visitor is included in the sample which is used to generate funnels.	

Streaming

For event streaming, the Research Council uses Vbrick Systems Inc. and YouTube. Use of these features is covered under the respective privacy statements of the companies supplying these services.

Social media

Research Council webpages contain links to our Facebook and Twitter profiles. Use of these features is covered under the respective privacy statements of the companies supplying these services.

Data processors for our webpages

EVRY is the supplier of operational and maintenance services for our main website, www.forskningsradet.no, and is the data processor in this capacity. As suppliers of analytic tools used on the site, Google Analytics and Hotjar are also data processors.

Bouvet and Redpill Linpro provide operational and maintenance services for the www.nysgjerrigper.no website, and are data processors in that capacity.

Hyper and Ravn Webveveriet provide operational and maintenance services for the www.forskningsdagene.no website, and are data processors in that capacity.

Contact with the Research Council

Newsletters

It is possible to subscribe to newsletters from the Research Council. Names and email addresses are stored in order to ensure that communications are sent to the correct subscribers. These data are stored in a separate database. You can unsubscribe from the service either via the website or a link in the newsletter.

The Research Council uses APSIS as its data processor for administering and sending out its newsletter and similar information. APSIS administers the database where email addresses are stored. We also use Oracle Webcenter Sites to manage subscriptions and send out newsletters. In connection with the Health&Care21 monitor, the Research Council uses MailChimp as HYPERLINK "http://as"data processor.

Personal data stored in connection with newsletter subscriptions are deleted when a user unsubscribes from the service.

Event registration

The Research Council uses an external registration system by Pindena in connection with registration for various events. In addition, we have entered into framework agreements with three event management agencies, Congress Conference, Conventor and Medvind AS, who handle event registration for us using their own registration systems. The information provided by registrants is stored for the purpose of administering registrations, participant services/communications and post-event evaluations.

Surveys/data collection

The Research Council uses the survey tool, SurveyXact, in connection with questionnaire-based surveys and other data collection activities targeting users of our services.

The Research Council also uses Kantar as supplier and data processor in connection with questionnaire-based surveys conducted among our users. Kantar has access to the survey responses which are made available to the Research Council in an anonymised format. After the survey has been conducted and the relevant agreement concluded, Kantar deletes the responses within two years or earlier if instructed by us to do so.

Survey participation is voluntary, and it is easy for recipients of survey invitations to opt out of receiving these requests in the future.

We process names and email addresses to manage survey invitations. The distribution list includes users of our services, newsletter subscribers and event registrants.

The basis for this data processing in part involves weighing the legitimate interest of improving performance of our tasks as a national executive body for strategic research management, to best serve the interests of our users and society at large, and in part an assessment of how this activity aligns with other primary purposes for personal data collection. More information about this is available upon request.

Nysgjerrigper magazine subscriptions

It is possible to register an individual Nysgjerrigper membership and subscribe to the Nysgjerrigper magazine (although classroom subscriptions are the most common subscription type). Names and email addresses must be collected for membership administration and in order to ensure that magazines are sent to the correct subscribers. Date of birth is also registered to determine the age of members. Members under 18 must also provide the name(s) and telephone number(s) of parent(s) or guardian(s). This information is used solely for the purpose of membership administration. The data are stored in a separate database and are not shared with others. Members must themselves cancel these services if they no longer wish to take part.

Digital adviser

The Research Council has a tool called “Digital adviser” which uses the Google Maps API to indicate event locations. Use of this service entails processing of personal data, with Google acting as the data processor for the Research Council, cf. Google’s Privacy Policy statement, which applies for this activity.

Requests for access to public documents

With regard to access to public documents, personal data are disclosed in accordance with the Freedom of Information Act and the Public Administration Act.

Special security measures and routines have been implemented for highly confidential information stored in the archive, such as sensitive personal data.

The Research Council is required to make its public records available to the public via the Internet, using the eInnsyn joint publication service for government agencies and the City of Oslo. Section 7 of the Regulations relating to the Freedom of Information Act, as referred to in Section 6, paragraph 4, specifies certain categories of information that are not to be made public in public records and journals published on the Internet. It has also been stipulated that the names of individuals must not be retrievable from eInnsyn after one year.

Statistics and analysis

One of the main tasks of the Research Council is to serve as an advisory body for the Government and ministries on research policy issues. This requires an extensive knowledge base in the form of statistics and analyses. Therefore, the Research Council has established a data warehouse that retrieves data (including personal data) from its eSøknad online submission system, the case handling and archive system, the ERP system and the national Current Research Information System in Norway (CRIStin). The data warehouse is used to compile reports, overviews and statistics related to R&D grant allocations. The data warehouse is also the source of published information on applications and projects. The names and titles of project managers for projects allocated funding, along with the project summaries, are published on the Research Council’s website and in the Project Databank as well as the Agency for Public Management and eGovernment’s (Difi) dataset repository.

Applicant institutions have access to information concerning their own applications and projects, including the names and titles of project managers, whether or not their proposals have been awarded funding. Other data retrieved from the data warehouse are always presented as aggregates.

The Research Council is the data controller for personal data processed in connection with efforts to collect, prepare, develop and make available R&D statistics on Norway. The Nordic Institute for Studies in Innovation, Research and Education (NIFU) prepares the R&D statistics and acts as data processor in the processing of personal data needed in these efforts. The Research Council and NIFU have entered into a written agreement regulating data processing activities.

The following information is processed as part of the compilation of registries:

- The Research Personnel Register: name, information about the individual’s position (title, position code and percentage of full-time equivalent), institutional affiliation (institution/faculty/department/institute), subject area, degree, discipline, year and place of university degree, doctoral degree and the year of defence of doctoral dissertation. The data are collected each year from universities, university colleges, research institutions and hospitals.
- The Doctoral Degree Register: name, gender, age, nationality, education (university or equivalent), educational institution, year of degree conferral, type of degree (title), year/month of dissertation defence, degree-conferring entity (institution/department), subject area for the degree. These data are collected twice a year from degree-conferring institutions and from the Research Council’s case handling system, which provides an overview of the fellowship positions funded by the Research Council.
- Personal data stored in the Research Personnel Register and the Doctoral Degree Register may only be disclosed to research organisations that are approved as research organisations in accordance with the Research Council’s criteria, and may only be used for statistical, research and analytical purposes.

Applicants for a position or employees at the Research Council

The Research Council processes personal data on its employees for the purpose of payroll and personnel administration. These data are managed in centralised systems to ensure employee rights, to fulfil the Research Council’s duties and obligations as an employer and to enable you to do the job you have been hired for. The Research Council registers information necessary for payroll disbursement, for example, basic data, salary level, timesheets, tax rate, tax municipality and union membership. Other information collected about employees is used in connection with job descriptions and facilitating work activities.

If you apply for a position at the Research Council we will need to process personal information to evaluate your application.

Your personal data are processed by the Research Council’s IT systems. We may also have information about you on physical records (documentation). The use of access cards, IT systems and digital tools, etc. will also be recorded by our systems.

All job applications are entered into in the Research Council’s mail journal and stored in an archive for approximately one year before being destroyed. Journal information is not deleted, but is protected in the electronic public record archive (i.e. the individual’s/applicant’s name is not included). Exceptions apply for job applications at the department director level, which are kept on record.

The routines for deleting personal data follow the Accounting Act (Regnskapsloven) and the Act relating to archiving (Arkivlova).

For documentation that has a permanent impact on employment or salary, the Research Council is subject to archiving requirements under the Act relating to archiving. In essence, this means that personal data may not be deleted without a statement from the National Archives of Norway. This also applies when you no longer work for the Research Council.

All past and present employees have a personnel folder in our archives. This includes job applications and other documents.

Personnel folders are to be preserved (i.e. job applications are not to be deleted or shredded). Personnel folders are cleaned out when the work relationship is concluded.

Access to personnel folders is only granted for work-related purposes.

Employees' personal data are primarily processed using the following systems (the list is not exhaustive):

HR Manager

This is the electronic recruitment system used to process information about persons applying for a position at the Research Council. The solution is supplied and operated by HR Manager Talent Solutions International, which acts as the system's data processor.

Case handling and archiving system

The system is used to administer employment and personnel-related issues. A personnel folder is created within the system for new employees to store documents of relevance for employment conditions and pensions.

Access monitoring

Personal information will be registered in our access monitoring system to provide you with access to the Research Council's office and facilities using your employee ID card.

Crisis management system

Security and preparedness management system. Personal information will be registered in the system so that we may contact you promptly in case of emergency or other critical situation.

Financial and personnel system

Personal data are processed in this system to safeguard your rights and obligations relative to salary, holiday, time off in lieu of pay and more.

Office 365

Interactivity solutions. Personal data are utilised to provide you with access to systems such as Sharepoint.

Travel

Personal information will be processed for reservations related to business travel.

Other IT systems where employees' personal data are processed:

- email;
- telephone and videoconferencing;
- case management and orders to the operations department;
- telephone switchboard – routing calls;
- case management system;
- room booking and time planning.

In addition, personal information may be handled by systems used in connection with specific roles or services at the Research Council, such as the following:

- tools for recording and publishing;
- web conferencing;
- tools for recording, streaming and publishing;
- system for breaches;
- administration of and support for research projects.

Safeguarding personal data security

We safeguard personal data by administering them in keeping with our internal procedures for information security, and our procedures for how we process them.

Our procedures govern how we organise work activities with regard to information security; how we carry out secure data storage, encryption or masking; how we establish and restrict access to data or physical locations; communicate, adapt related procurements, follow up respective suppliers and manage any issues that arise. The main, definitive rule is that access to personal data is only provided to persons with a concrete need for such access in connection with their work for the Research Council.

We conduct regular risk and vulnerability assessments of our activities related to personal privacy, information security and of the IT systems we use, and use the results of these analyses to adjust how we work. Our efforts are supported by our department for internal revision and our Data Protection Officer.

Sharing of personal data with others

The Research Council shares personal data with its data processors, other data controllers and other public agencies. This is done on the basis of data processor agreements, agreements on shared data controller responsibility, legislation/regulations or other corresponding legal grounds.

If we are processing data outside Norway but within the EU/EEA, personal privacy is protected through compliance with the Personal Data Act, regulations relating to personal privacy within the EU/EEA and any relevant nation-specific regulations in the area.

If we are processing personal data outside the EU/EEA we take additional steps to protect personal privacy by only transmitting personal data to parties that: receive and process data in a country that is previously recognised by the European Commission to provide an adequate level of data protection, are subject to or have signed a data processor agreement containing standard contractual clauses for data transfers between EU and non-EU countries or similar provisions, or that have prior certification through the EU-U.S. Privacy Shield Framework.

We check that those parties with which we share personal data process the data in accordance with the statutory framework and the purpose of the data sharing.

Our obligations

When processing data we are first, among other things, obligated to:

- have a reasonable, necessary purpose for the activity
- ensure a fair and lawful basis for data processing
- provide information about the activity that is concise, transparent, intelligible and easily accessible;
- create a framework that enables registered individuals to exercise their rights;
- rectify inaccurate or incomplete information;
- erase information after it has served its purpose when further storage is not required by the statutory framework;
- conduct a Data Protection Impact Assessment when the processing activity is likely to result in a high risk to the rights and freedoms of the registered individuals;
- implement data protection principles in the development of our services and solutions (data protection by design and default);
- establish internal controls to ensure and demonstrate that compliance with the Personal Data Act, and safeguard personal data on record;
- document the processing activities where we act as data controller or data processor;
- enter into a data processor agreement when using or acting as a data processor;
- handle breaches arising in connection with data processing, report breaches to the Norwegian Data Protection Authority when and as we are statutorily obliged to, while ensuring adequate information to the registered persons affected;
- safeguard the protection of personal privacy if and when we undertake international transfers of personal data.

As a public agency we are required to have a Data Protection Officer who is to be informed of our activities on an ongoing basis and who works to safeguard the interests of registered users and acts as liaison with the Norwegian Data Protection Authority.

Your rights

You have the right to:

- access the information we have on record for you;
- rectification or completion of inaccurate or incomplete information;
- erasure of your data if they have been processed unlawfully (please note, there are exceptions to this right, for example, when legislation requires that we continue to store data).
- restriction of data processing pending clarification of a question regarding the legal basis, to reach a decision regarding an objection to data processing, or to delay/restrict data erasure.
- withdraw your consent if you initially granted it to us as the basis for a data processing activity;
- object to the data processing if it is not based on consent, agreement or legal obligation; if the processing is carried out in the public interest or as an exercise of official authority (GDPR Art. 6 (1) litra e), or in the pursuit of legitimate interests (same article, litra f), and the processing is not necessary for the protection of vital interests. You may at any time object to direct or targeted marketing.
- data portability in a structured, commonly used, machine-readable format if the data processed were based on consent/agreement and you are the one who has provided them to us. We will only release data when able to confirm your identity, secure the data using encryption, and ensure that doing so does not infringe on the rights or freedoms of others. The information will be transmitted free of charge unless we can prove that the cost is unjustifiable or excessive (please note, however, that this right is primarily intended to protect customers in commercial matters such as switching between service providers, and will only be applicable to our activities in certain cases);
- information about our processing of personal data that is concise, transparent, intelligible and easily accessible.
- Not to be subject to a decision based solely on automated processing that is wholly automated (i.e. independent of human influence) and produces legal effects concerning you (i.e. controlling your rights or obligations). This does not apply, however, unless the decision is based on consent, is necessary for entering into or performance of a contract, or is based on legislation that safeguards the interests of the individual. In the case of such decisions we will implement measures to safeguard your interests, and you will have the right to express your point of view, to contest the decision and to obtain human intervention.

When you contact us to exercise your rights we will respond without undue delay, and within 30 days at the latest.

Please note that in certain circumstances your rights may be limited by terms or requirements we are subject to under legislation/regulations or for corresponding legal reasons. We will evaluate this specifically and inform you about this each time you contact us to exercise your rights.

Contact us with questions about privacy

If you have any questions regarding our processing of personal data or if you wish to exercise your rights, please contact the Research Council at:

email: post@forskningsradet.no

telephone: +47 22 03 70 00

mailing address: Research Council of Norway, P.O. Box 564 NO-1327 Lysaker

The Data Protection Officer at the Research Council works to safeguard the personal privacy of all individuals whose data we process, to provide advice on our obligations and your rights, and serves as a liaison with the Norwegian Data Protection Authority. You may contact our Data Protection Officer by email at personvern@forskningsradet.no.

If you are looking for further information regarding personal privacy and its related regulations in English, we recommend you consult the following international web pages as sources:

The European Data Protection Supervisor[lenke slutt], which is the EU's independent data protection authority.

The Information Commissioner's Office, which is the United Kingdom's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Complaints about our processing of personal data?

The Norwegian Data Protection Authority is the supervisory authority for our processing of personal data.

For questions regarding our processing of personal data, the Norwegian Data Protection Authority recommends that you contact us first to try and clarify the issue. If you are not satisfied with the clarification and wish to lodge a complaint, the Norwegian Data Protection Authority recommends that you then contact our Data Protection Officer.

If after having contacted our Data Protection Officer you still wish to lodge a complaint about what you see as a breach in our processing of personal data, the Norwegian Data Protection Authority website provides information on how to contact the Norwegian Data Protection Authority for assistance.

Published 25.04.2019 | Last updated 25.04.2019 | Download