Privacy statement

In this privacy statement, we describe how the Research Council of Norway processes personal data.

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).

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. The date of the most recent page update can be found at the bottom of the page.

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 meet:

- the overriding objectives and duties that we have been ordered to fulfil pursuant to the Regulations relating to the Research Council's statutes;
- 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 job 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.

What types of personal data do we process?

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

Examples of the types of personal data collected for processing include name, address, telephone number, email address, personal 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 our policies and procedures. Most relevant in this context are the policy for the protection of personal privacy, the policy on security, the policy on processing of personal data and our procedure for 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 Norwegian Archives Act (Arkivlova) and pertaining regulations.

More information about privacy protection is provided below by topic:

Application processing and project assessment and follow-up

Personal data processed in connection with application processing, in the assessment and follow-up of projects that have been granted funding, and when in monitoring the use of allocated funding through 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 primarily consists of name, national identity number, email address, position, place of employment and role in relation to the project. For employees, referees, and members of the Executive Board, Programme Boards and Division Research Boards and others receiving remuneration from the Research Council, information necessary for disbursing the remuneration, such as national identity number (or D-number if relevant), will also be stored in the registry. For referees, information linked to previous involvement in application assessment is also recorded.

Persons 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.

For referees, information relating to previous assessment assignments will also be registered. To find new referees, several external online sources are often used, including: Expert Lookup, Google Scholar author search tool, Pindena, Web of Science and Scopus.

Expert Lookup uses artificial intelligence to assist in the selection of the right experts. The purpose is to ensure the best possible match between the topic the research projects aims to elucidate and the referee panel's expertise and impartiality. The final decision on which experts to appoint and which referee panel will assess the application will be decided on the basis of manual assessments carried out by the Research Council. The Research Council enters selected information in a secure and user-driven API provided by Elsevier. The Research Council uploads the project title, project summary, objectives, project number and the name of the project manager. The API is the line of communication between the Research Council's database and Elsevier's database. The API transfers the information the Research Council wishes to enter in Expert Lookout. Based on the information selected by the Research Council, Expert Lookup creates a semantic fingerprint that is used in a search to find a certain number of relevant experts that can potentially serve as members of a referee panel for one or more applications. The uploaded information is matched against Elseviers's own database (Scopus), which contains large amounts of information and data based on publicly available information, including information about publications and academic background. A hit/no-hit function is used. The Research Council is given access to Expert Lookout and

the solution's results through a Webclient (URL link) that is user-driven through a password and user name.

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 that prevents the data from being linked to individual persons. These data are collected for the purpose of 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 Google Analytics privacy protection guidelines 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 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

Epinova and Optimizely is the supplier of operational and maintenance services for our main website, www.forskningsradet.no and www.nysgjerrigper.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.

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

Newsletters

It is possible to subscribe to electronic newsletters from the Research Council. Email addresses are stored to ensure that the newsletters are sent to the correct subscribers.

No other information is required, but may be provided subject to the recipient's consent.

You can unsubscribe from the service either via the website or a link in the newsletter.

The Research Council, Nysgjerrigper Science Knowledge Project and National Science Week (Forskningsdagene) uses Microsoft Dynamics 365 as its data processor for administering and sending out its newsletters and similar information. The data about newsletter subscribers are also stored in the Research Council's CRM system, Microsoft Dynamics 365. The purpose of processing personal data in the CRM system is to maintain and update contact information.

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

Event registration

The Research Council uses an electronic registration system from 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 people registering for an event is stored for the purpose of administering registrations, participant participation and post-event evaluations.

The data from Pindena are also stored in the Research Council' CRM system, Microsoft Dynamics 365. The purpose of processing personal data in the CRM system includes maintenance and updating of contact information, mapping and analyses of activities and events offered to users of the system, and necessary administration of events (including documentation of participation) and mobilisation.

Surveys/data collection

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

The Research Council also uses Kantar as a supplier and data processor in connection with questionnaire-based surveys conducted among the users of our services. 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.

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 be able to send survey invitations. We retrieve the names and email addresses from our register of the users of our services, our register of newsletter subscribers, and people who have registered for our events, and from the CRM system.

The legal basis for the processing is a legitimate interest pursuant to GDPR Article 6(1) letter f). The Research Council may only process personal data if necessary for the purpose of pursuing a legitimate interest that overrides the interest of the data subject. We consider that the interest of improving the performance of our tasks as a national executive body for strategic research management is a legitimate interest, and also in the interest of our users and society at large. In our opinion, this legitimate interest overrides the interest of the data subject. More information about the weighing of interests is available on request.

Data about referees recruited via Microsoft Forms are stored in the Research Council's CRM system, Microsoft

Dynamics 365, for maintenance and updating of contact information for up to five years from the date of registration.

Participation in the Nysgjerrigper Science Competition

Pupils and teachers in grades 1-7 can participate in the Nysgjerrigper Science Competition by submitting a research report along with the teacher's and school's contact information. Filemail AS is used as a data processor to receive the teachers' contact information and files with the pupils' research reports. As the data controller, the Research Council has entered into a data processing agreement with Filemail AS. Filemail AS deletes all data in accordance with our instructions. Data will be deleted from Filemail after the projects have been processed by the Research Council. The following information is collected in order to process contributions and carry out the Nysgjerrigper Science Competition: Name, email address, IP addresses, workplace and telephone number. It is optional for teachers to use Filemail to participate in the competition.

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, addresses 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). Members must cancel their own membership if they no longer want to be a member/subscriber.

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 procedures have been implemented for information stored in the archive that needs special protection, such as special categories of personal data.

The Research Council is required to make its public records available to the public via the internet, using the Electronic Public Records (OEP) /eInnsyn services. The Regulations relating to the Freedom of Information Act Section 7, cf. Section 6 fourth paragraph, specify certain categories of information that are not to be made public in public records and records published on the internet. It is also stated that the names of individuals must not be retrievable from OEP/eInnsyn after one year.

Statistics and analysis

One of the main tasks of the Research Council is to serve as an advisory body to 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 our electronic application system, the case management 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, and these data are used in an aggregated form for analytical purposes. 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, regardless of whether or not their proposals have been awarded funding.

The Research Council is also the data controller for personal data processed in connection with efforts to collect, prepare, develop, present and make available R&D statistics for 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 doctoral degree-conferring institutions and from the Research Council's case management 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 approved 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 with the Research Council and the Research Council's employees

The Research Council processes its employees' personal data 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 to do. The Research Council registers information necessary for payment of salary, for example basic data, salary level, time sheets, 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 job with the Research Council, we need to process information about you to be able to consider your application.

Your personal data are processed by the Research Council's IT systems. We may also have information about you in printed documents. You will also leave electronic traces when you use your access card, our IT systems and digital tools, etc.

All job applications are entered into the Research Council's mail journal and stored in an archive for approximately one year before being destroyed. . Information in the records is not deleted, but is protected in the Electronic Public Records (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 procedures for deleting personal data comply with the Accounting Act (Regnskapsloven) and the Archives Act (Arkivlova).

For documents that have a permanent impact on employment or salary, the Research Council is subject to an archiving duty pursuant to the Archives Act, which means that personal data can in principle not be erased without the consent of 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 will not be deleted or shredded). Personnel folders are reviewed and emptied 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 with the Research Council. The solution is supplied and operated by HR Manager AS, which acts as the system's data processor.

Case management and archiving system

The system is used to administer employment and personnel-related cases, among other things. A personnel folder is created within the system for new employees to store documents of relevance to the employment relationship and pension.

Access monitoring

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

Crisis management system

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

Financial and personnel system

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

Office 365

Interactive solution. Your personal data are processed to give you access to e.g. Sharepoint.

Travel

Personal information about you will be processed to be able to book business trips.

Other IT systems where employees' personal data are processed:

- email solution;
- telephone and video conferencing solution;
- case management system for processing cases and orders to the operations department;
- telephone switchboard – routing calls;
- case management system;
- room booking and time planning system.

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

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

Safeguarding personal data security

We safeguard personal data by administering them in keeping with our internal information security procedure, and our procedures for the processing of personal data.

Our procedures govern how we organise work activities with regard to information security; how we carry out secure data storage, encryption or masking; 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 we process personal data, we have a duty to, among other things,

- determine a reasonable and necessary purpose for the processing;
- ensure a correct legal basis for the processing;
- provide information about the processing in a concise, transparent, understandable and easily accessible manner;
- enable data subjects to exercise their rights;
- correct information that is incorrect or incomplete;
- delete data when the purpose has been fulfilled and we are not required to further store data by law/regulations;
- carry out a data protection impact assessment when it is likely that the processing may entail a high risk to the rights and freedoms of the data subjects;
- take privacy into account when developing our services and solutions (privacy by design);
- establish internal control to ensure and show that we comply with the Personal Data Act;
- ensure the information security of registered personal data;
- keep records of processing activities for which we are the controller or data processor;
- enter into a data processing agreement when we use a data processor or are data processors ourselves;
- handle deviations that arise in connection with the processing, report deviations to the Data Protection Authority when and as we are required to do so, and ensure information for the affected persons, and
- safeguard privacy if we transfer data abroad.

As a public body, we are obliged to have a data protection officer who is to be informed of our processing on an

ongoing basis and who works to safeguard the interests of data subjects and acts as liaison with the Norwegian Data Protection Authority (Datatilsynet).

Your rights

You have the right to (please see the Norwegian version of this page to access links to more information on the points below)

- access the information we process about 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) letter e), or in the pursuit of legitimate interests (same article, letter 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 processing 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 laws/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

Tel.: +47 22 03 70 00

Post: 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.

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 of regulations in our processing of personal data, the Norwegian Data Protection Authority website provides information on how to lodge a complaint with the Norwegian Data Protection Authority.

Published 25 Apr 2019 | Last updated 28 Jan 2025