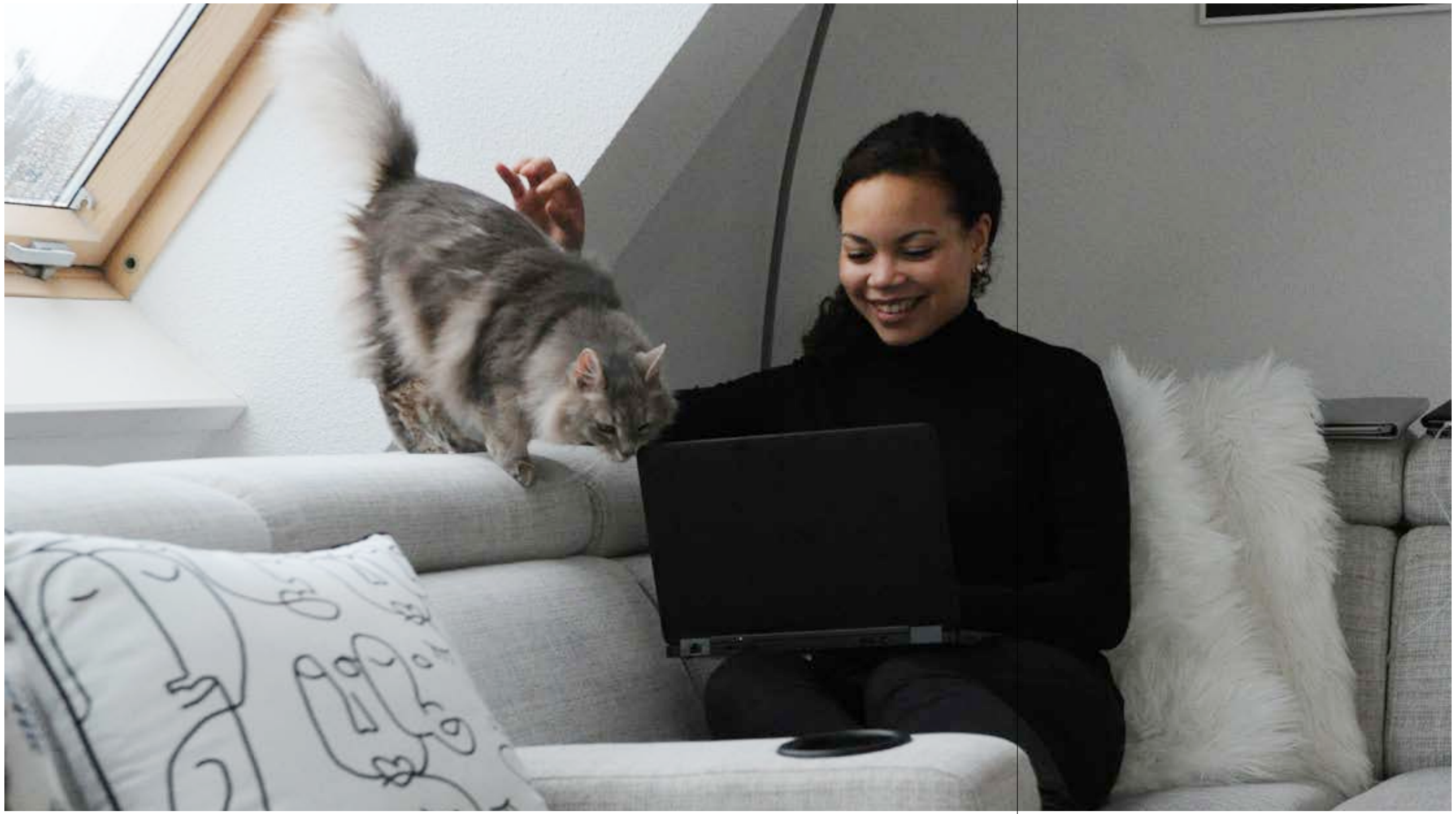
Ministry of Economic Affairs
and Climate Policy

INFORMATION SECURITY AND PRIVACY

Suppliers guide offering information about:

what we expect from you as a supplier

the approach to information security and privacy at EZK



Protecting information and personal data is the top priority for the Ministry of Economic Affairs and Climate Policy (EZK). That requires significant effort from our own employees, but also from our suppliers. You can read more about it in this concise guide.

The Ministry of Economic Affairs and Climate Policy (EZK) aims to be a safe and secure organisation that safeguards the interests and rights of our citizens and society. We ask the same of our employees, our agencies and our suppliers. This guide provides a concise summary of the information security and privacy policies at EZK. As our supplier, we expect you to comply with the same principles as we do. Only then can we safeguard information security and privacy throughout the chain. Other specific requirements for information security and privacy are set out in the supplier agreement.

Vision on information security

EZK champions a future in which our objectives are optimally achieved in a secure, reliable environment. This environment provides scope for new technological developments and facilitates innovative applications. We will create this future by leveraging our information security in smart ways and ensuring that it keeps pace with developments. This is how we will achieve information security at the source, robust access security and an infrastructure that facilitates new technological applications. The information security organisation supports the overall organisation by offering up-to-date insights into opportunities and threats.

The goal is to protect the availability, integrity and confidentiality of the information supply and to ensure that personal data is processed with due care

Vision on privacy

Data from citizens and about citizens must be safe with EZK, and citizens' privacy must be guaranteed. That means that EZK must handle personal data and other data in a way that is both sustainable and reliable. Apart from complying with laws and regulations, EZK aims to be a reliable partner that processes personal data relating to its public tasks securely and responsibly. In terms of information security and privacy at EZK, the aim is to protect the availability, integrity and confidentiality of the information supply using an approach based on risk management. This, in turn, safeguards the continuity of operational processes and reinforces citizens', businesses' and other government bodies' confidence in the ministry.

Regulatory framework

We ensure compliance with the following laws and standards:

- Government Information Security Baseline (BIO)
- General Data Protection Regulation (GDPR)
- ISO standard 31000 (risk management)
- ISO 27001
- ISO 27002
- Civil Service Information Security Regulations 2007 (VIR 2007)
- Civil Service Information Security (Classified Information) Regulations (VIR-BI 2013)

Management and accountability at EZK

At EZK management and accountability have been structured by means of the following instruments.

- A quality cycle has been introduced in the area of information security and privacy.
- The ministries are audited by the Netherlands Court of Audit and the Central Government Audit Service (ADR).
- Our systems, processes, employees and suppliers are audited by independent parties in order to ensure the continued safeguarding of security and data protection.

National security and ICT/data security are top priorities

Organisational measures

EZK uses various organisational measures to safeguard security and privacy. A number of examples are provided below.

- Information security is part of the security officer's (BVA) integrated security policy.
- Employees and external parties are granted access to information and information systems only after authorisation by the competent person or institution.
- We operate on the basis of the 'need to know' principle and ensure that authorised persons are made aware of information security and privacy issues.
- We focus on privacy by design and security by design.
- National security with regard to Dutch society, the security of data and information and communication technology (ICT) and the privacy of our citizens and employees are top priorities.
- The Privacy Impact Assessment (PIA) is used to assess privacy risks for the organisation at an early stage.
- Access to digital systems must be controlled using strong passwords, two-factor authentication and password managers.

Utilising opportunities, such as deploying new technologies, involves taking risks. It is important to find the right balance in this regard. Risk management is a continuous process in which risks are identified and the possible impact is determined. Together, we can safeguard the security of data and systems by mapping out risks in a structured manner and by taking measures to mitigate them. We ask you to adhere to the same measures and principles as those outlined in this guide. By doing so, we can safeguard the security and privacy of data and processes. We only process personal data if there is a legal basis for doing so. We put the data subject first. Personal data is retained for no longer than strictly necessary to achieve the purpose for which the data was collected. Make sure that personal data is accurate and up to date, and be cautious about providing data to third parties. ■

Do you still have questions?
If you still have questions about information security and/or privacy, such as questions about procedures or how measures should be interpreted, you can always notify your contact person at EZK. More information about specific requirements is also provided in the contract or agreement.

Explanatory notes

Stronger together: Information security and privacy at EZK

The Ministry of Economic Affairs and Climate Policy (EZK) values public-private partnership in which central government and private companies work together to leverage opportunities that benefit the economy and society, such as carbon neutrality, a strong digital economy, and the transition to circular agriculture. EZK has expressed an ambition to use efficient, cutting-edge information and communication technologies so that it can fulfil its tasks and responsibilities, such as optimising support for citizens and companies. Information security and privacy are indispensable in this regard.

Protecting interests

The interests to be protected, such as company secrets, personal data, confidential or **classified information**, and the safeguarding of continuity are top priorities for the ministry. This requires significant effort from our own employees, but also from the partners we work with. Failure to secure data sufficiently – or at all – and ICT failures lead to an unacceptable risk of reputation damage, financial damage or the loss of valuable data. This means that EZK and its partners must take measures to guarantee data security, so as to ensure citizens retain their confidence in the public administration system.

Laws, standards and measures

The government makes use of the Government Information Security Baseline (BIO). This is the **framework of standards** for information security used throughout the government, based on the latest internationally acknowledged ISO standards (**ISO 27001**). This baseline does not include the implementation guidelines; see the ISO 27002 for that information. In order to achieve the envisioned level of security for data, information systems and operational processes, three aspects are crucial. The importance of each aspect is assessed and the higher the outcome, the more crucial it is to take sufficient measures.

1. Availability, which can be guaranteed through good maintenance and by updating systems regularly. Back-ups and fall-back scenarios ensure that data access can be restored quickly in the event of a disruption.
2. Integrity, accuracy and completeness throughout the entire data life cycle. Whether it is en route or stored somewhere, data should not be susceptible to alteration by unauthorised parties (access management on a 'need-to-know' basis).
3. Confidentiality, which also relates to privacy. Taking measures to prevent data from falling into the wrong hands, while allowing the right people to access it.

The processing of personal data – data that can be traced by to an identified or identifiable natural person – is subject to the General Data Protection Regulation (**GDPR**) and the **General Data Protection Regulation (Implementation)** Act. To meet the requirements of this legislation, **the ministry** has formulated a privacy policy. As the data controller, EZK always remains responsible for the processing of personal data, but the GDPR also sets requirements for partners (**data processors**). EZK applies **privacy by design and default** in this regard and asks its partners to do the same. Organisational and technical measures must be in place to ensure that personal data is processed with due care. Central government is transparent about how it processes personal data. The **GDPR register** offers an overview of the types of data concerned, why the data was collected, what will be done with the data and who is responsible for processing it.

Roles and responsibilities

Improving resilience to potential threats or risks is an ongoing process ('plan, do, check, act') and it starts with explicitly engaging in mutual dialogue about roles and responsibilities. The main objective is to effectively minimise actual risks. The minimum level of security (for example, the **BBN BIO baseline assessment, which assesses network and information systems security according to the Government Information Security Baseline**) has been agreed and clearly recorded. Agreements have been laid down in more detail in a Service Level Agreement (SLA). If a partner processes personal data on behalf of EZK (the data controller), then the ministry for which the personal data is processed drafts a **data processing agreement**. This agreement sets out a range of details, such as the purposes for which data may be processed, how data must be secured, and the stipulation that data may only be shared within the context of the predefined purposes. Deviations are actively reported and are part of a periodic evaluation. Performance is verifiable and serves as proof of the contractually agreed quality (and level of security). Additional security measures for preventative purposes may also be agreed upon. Agreements are made regarding the provision of information about disruptions and cybercrime risks, preferably in real time. This makes it possible to respond promptly to newly emerging threats, risks and incidents. A data breach on the part of a data processor that will probably present a risk to 'the rights and freedoms of data subjects' is a notifiable incident, for example. In such a situation, EZK, as the data controller, must notify the Dutch Data Protection Authority immediately (within 72 hours). Suppliers must disclose their supply chain of secondary suppliers and be transparent about the measures they have taken to ensure that their suppliers comply with the requirements that were initially imposed on them. EZK has the right to conduct an audit at all times, or to have such an audit conducted, and partners will conduct an (internal or external) audit of the most significant risks at least once a year. ■

This is a publication of:
Ministry of Economic Affairs and Climate Policy

Address for visitors
Bezuidenhoutseweg 73
2594 AC The Hague
Telephone number: +31 (0)70 751 8911

Postal address
P.O. Box 20401
2500 EK The Hague

https://www.government.nl/ministries/ministry-of-economic-affairs-and-climate-policy