Draft Data Processing Agreement (ARVODI 2025)

Information campaign 'Working in the Netherlands' for the Dutch Ministry of Foreign Affairs Embassy of the Kingdom of the Netherlands in Warsaw, Poland.

Contract number: 201865005.011.087.

The undersigned:

1. The State of the Netherlands, which has its seat in The Hague,
represented by the Minister **OR** State Secretary of/for [portfolio],
legally represented in this matter by
[signatory's name and position]
hereinafter referred to as 'the Contracting Authority',

and

2. [Contractor's full name and legal form],
which has its registered office in [...],
legally represented in this matter by
[signatory's name],
hereafter referred to as 'the Contractor',

WHEREAS:

- In so far as the Contractor processes Personal Data for the Contracting Authority in the context of the Contract, the Contracting Authority qualifies as a Controller for the Processing of Personal Data and the Contractor as a Processor;
- The Parties to this Data Processing Agreement, as referred to in Article 28, paragraph 3 of the Regulation, wish to record their agreements on the Processing of Personal Data by the Contractor.

AGREE AS FOLLOWS:

Article 1. Definitions

Certain terms in this Data Processing Agreement are written with initial capitals. These terms are defined in the ARVODI 2025 or the Regulation, on the understanding that the definitions of a number of terms are geared to the Data Processing Agreement. In addition thereto, the following terms are thus defined below for the purposes of this Data Processing Agreement, regardless of whether they are used in the singular or plural or as verbs or nouns:

1.1 ARVODI 2025: the General Government Terms and Conditions for Public Service Contracts 2025.

1.2 Data Subject: the person whom the Personal Data concerns.

1.3 EEA: the European Economic Area, comprising all EU countries in addition to Liechtenstein, Norway and Iceland.

1.4 Personal Data Breach: a breach in security that leads to the accidental or unlawful destruction, loss, change or unauthorised disclosure of, or unauthorised access to, data that has been transferred, stored or Processed in any other way.

1.5 Recipient: a natural or legal person, public authority, agency or another body, to which the Personal Data is disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or member state law are not regarded as Recipients; the Processing of that data by those public authorities takes place in compliance with the data protection rules applicable to the purposes of the processing.

1.6 Contract: the agreement between the Contracting Authority and the Contractor [title] dated [date], reference number [number].

1.7 Personal Data: any data concerning an identified or identifiable natural person that is Processed by the Contractor for the Contracting Authority in the context of the Contract.

1.8 Supervisory Authority: an independent public authority which is established by a member state pursuant to Article 51 of the Regulation.

1.9 Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.10 Processor: a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.11 Data Processing Agreement: this agreement including its recitals and the accompanying schedules.

1.12 Processing: any operation or any set of operations concerning Personal Data or any set of Personal Data, carried out in the context of the Contract via automated or manual procedures, including in any case the collection, recording, organisation, structuring, storage, updating or modification, retrieval, consultation, use, disclosure by means of transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data.

1.13 Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such Processing are determined by Union or member state law, the Controller or the specific criteria for its nomination may be provided for by Union or member state law.

Article 2. Object of this Data Processing Agreement

2.1 This Data Processing Agreement governs Processing by the Contractor in the context of the Contract and is inextricably linked to the Contract.

2.2 The nature and purpose of the Processing, the type of Personal Data and the categories of Personal Data, Data Subjects and Recipients are set out in Schedule 1.

2.3 The Contractor guarantees that the appropriate technical and organisational measures will be taken in order to ensure that Processing complies with the requirements of the Regulation and that the rights of the Data Subject are protected.

2.4 The Contractor guarantees compliance with the requirements of the applicable legislation relating to the Processing.

Article 3. Entry into force and term

3.1 This Data Processing Agreement enters into force as soon as it has been signed by the Parties.

3.2 This Data Processing Agreement terminates after the Contractor has erased or returned all Personal Data and has deleted existing copies in accordance with article 10 of this Data Processing Agreement.

3.3 Early termination of this Data Processing Agreement is not possible.

Article 4. Scope of the Contractor's Processing competence

4.1 The Contractor will Process Personal Data only for, and on the basis of written instructions from, the Contracting Authority, unless the Contractor is required by a statutory regulation to carry out Processing. In that case the Contractor will notify the Contracting Authority of such a statutory regulation prior to the Processing, unless that statutory regulation prohibits such notification on important grounds of public interest.

4.2 The Contractor has no control over the purpose or means of the Processing within the meaning of the Regulation.

Article 5. Security of the Processing

5.1 Without prejudice to article 2.3 of this Data Processing Agreement, the Contractor will implement the technical and organisational security measures described in Schedule 2.

5.2 The Parties recognise that guaranteeing an appropriate level of security may require additional security measures to be implemented on an ongoing basis. The Contractor guarantees a level of security appropriate to the risk.

5.3 At the express written request of the Contracting Authority, the Contractor will adopt additional measures to ensure the security of the Personal Data at the expense of the Contracting Authority.

5.4 The Contractor will not Process any Personal Data outside the EEA unless it has obtained express written consent from the Contracting Authority to do so, subject to further conditions if necessary, and barring statutory obligations to the contrary.
After obtaining the consent of the Contracting Autoritty, the Contractor may process personal data:
1). In another country recognised by the European Commission as providing an adequate level of protection of personal data;
2). In a country other than those referred to in point 1)., articles 44-47 of the GDPR apply.

5.5 The Contractor will inform the Contracting Authority without unreasonable delay as soon as it becomes aware of any unlawful Processing of Personal Data or failure in (or failure to comply with) the technical and organisational security measures referred to paragraphs 1 and 2.

5.6 The Contractor will assist the Contracting Authority in ensuring compliance with the obligations under Articles 32 to 36 inclusive of the Regulation.

Article 6. Duty of Confidentiality of the Contractor's Staff

6.1 The Personal Data is confidential as referred to in article 11.1 of the ARVODI 2025.

6.2 The Contractor guarantees that, as referred to in article 11.2 of the ARVODI 2025, its Staff have undertaken to observe the duty of confidentiality.

Article 7. Subprocessor

If the Contractor, with due regard for the provisions of article 6 of the ARVODI 2025, engages another Processor to carry out processing activities for the Contracting Authority, the other Processor must be bound by an agreement imposing the same data protection obligations as those imposed by this Data Processing Agreement.

Article 8. Assistance concerning rights of Data Subjects

8.1 Taking into account the nature of the Processing, the Contractor will assist the Contracting Authority by means of appropriate technical and organisational measures, in so far as this is possible, in the fulfilment of the Contracting Authority's obligation to respond to requests for exercising the Data Subject's rights laid down in chapter III of the Regulation.

8.2 Each of the Parties will bear any costs they incur in connection with paragraph 1.

8.3 The Contractor will send a request from a Data Subject to the Contracting Authority as soon as possible.

Article 9. Personal Data Breach

9.1 The Contractor will inform the Contracting Authority, without unreasonable delay, as soon as it becomes aware of any Personal Data Breach, in accordance with the agreements set out in Schedule 3.

9.2 After reporting an incident as described in paragraph 1, the Contractor will also inform the Contracting Authority of developments relating to the Personal Data Breach.

9.3 Each of the Parties will bear any costs they incur in relation to the Personal Data Breach.

Article 10. Return or erasure of Personal Data

10.1 Once the Contract expires, the Contractor will erase the Personal Data or return it to the Contracting Authority, whichever the Contracting Authority prefers. The Contractor will delete any copies, barring statutory rules to the contrary. The Processor shall not be obliged to erase or return the personal data where national and European law requires it to continue to store the personal data, regardless of the expiry or termination of this Agreement. Furthermore, the processor shall not be obliged to erase or return the personal data where the further processing of the entrusted personal data is necessary for the purposes defined in the article 5.1 e of the GDPR.

10.2 The Personal Data will be returned to the Contracting Authority in the format and manner stipulated by the Contracting Authority.

Article 11. Obligation to supply information and audit obligation

11.1 The Contractor will provide all necessary information to show that the obligations set out in this Data Processing Agreement have been and are being fulfilled.

11.2 The Contracting Authority can perform an audit (or have an audit performed) of the Processing activities that fall under the Data Processing Agreement if concrete circumstances give reason to do so. The Contractor will cooperate fully with audits, including audits among the Contractor's Staff, unless it cannot reasonably be expected to do so.

11.3 The Contractor will immediately notify the Contracting Authority if, in its opinion, an instruction from the Contracting Authority in the context of article 11, paragraph 1 and/or paragraph 2 of this Data Processing Agreement breaches a statutory regulation relating to data protection.

11.4 The Parties themselves will bear the costs they incur in connection with the information provision and audits referred to in this article, including the costs of third parties engaged by them.

11.5 The Contracting Authority is authorised at all times to propose further measures prompted by the information obtained under this article. The Contractor is obliged to carry out these measures in so far as is reasonable.

The Hague, [date] [place], [date]

FOR THE MINISTER
/ STATE SECRETARY OF/FOR [Contractor's name]
[portfolio],

[signatory]

[signatory's name] [signatory's name]

Schedule 1 Processing Personal Data

The nature and purpose of the Processing activities, including the statutory basis	The Contractor is processing personal data in order to implement the following aims of the Contract: a). The 'Fair labour mobility campaign' (Part 1) aims to inform (potential) Polish mobile workers before departure about their rights and obligations in the Netherlands and where they can find assistance; b). The 'Posted workers NL' campaign (budget part 2) aims to inform Polish employers who post workers to the Netherlands and Polish self-employed persons who do business in Poland and provide services in the Netherlands about the applicable legislation on posting, in particular the notification system for posting. According to the requirement 36 of the Requirements and Declaration of agreement, The Tenderer must remain flexible to implement possible new requests that were not initially planned but which comply with the scope, requirements and financial constraints of the contract, during the whole duration of the contract. It means that the purpose of processing of data could be broadend. The Contractor is processing personal data only for the purpose of the Contracting Authority. The data are processing internally and, both automatically and manually.
Type of Personal Data	0 **Ordinary Personal Data** 0 Special categories of Personal Data - social media user data: first name, last name, nickname, image, content of statements (comments, messages), other data disclosed by the user, - targeted person data: targeting tags - gender - recorded person data: image, including audio image.
Description of Personal Data categories	- social media user data: first name, last name, nickname, image, content of statements (comments, messages), other data disclosed by the user, - targeted person data: targeting tags - gender - recorded person data: image, including audio image.

Description of categories of Data Subjects	The Contractor is processing data of social media users to implement information online campaigns.
Description of categories of Personal Data Recipients	Subprocessors, also outside the EU.

Subprocessor(s)

Subprocessor’s name and contact details	
Subprocessor’s commercial register number	
The subject matter/nature and purpose of the Processing	
The type of Personal Data	
Description of categories of Personal Data	
Description of categories of Data Subjects	
Description of categories of Personal Data Recipients	
Location of Personal Data Processing	
……..	

The information in the controller’s records, obligatory under Article 30 of the Regulation, can be used to complete this schedule.

Schedule 2 Appropriate technical and organisational measures

The Dutch Ministry of Foreign Affairs (BZ) is required to ensure that all processes and information systems comply with the Government Information Security Baseline (BIO) and the BZ Information Security Baseline 2021. Service providers that process BZ information must therefore meet the following additional requirements:

A. Staff reliability and security

☐ All staff with access to information relating to this agreement must have signed a non-disclosure/confidentiality agreement.

B. Product and system maintenance

☐ All products and systems used in executing the Contract, including the information and physical security systems, must be maintained in accordance with the manufacturer's recommended maintenance specifications. The systems must always be within the vendor lifecycle.

☐ System maintenance must be carried out as part of the change management process. A management method is used to keep a record of changes to the configuration.

☐ If the two above-mentioned maintenance requirements cannot be met for justified reasons, BZ must be informed accordingly and provided with a substantiated risk assessment.

☐ If the manufacturer has not supplied any specifications, international best practices must be applied.

C. System and web application hardening

☐ All systems must be hardened in accordance with the recommendations of the developer/manufacturer.

☐ Clearly defined change management procedures must be in place and must be applied for all changes.

☐ A backup[*] must be made of all systems and configurations covered by this agreement to protect them from loss or damage, including mitigating the risks of hostage software attacks.

☐ Applications (including web applications) may be developed/modified solely by developers who have been sufficiently trained in OWASP/CIS/NIST/NCSC web guidelines and mobile application development guidelines.

☐ The contractor is responsible for performing vulnerability scans[†] on the services provided. Any low risks detected (CVSS <3.9) must be resolved within one month. Medium risks (CVSS 4.0-6.9) must be resolved within a week and high/critical risks (CVSS >7.0) within 24 hours. If this is not possible, the Information Security Centre (i-SecurityCentre@minbuza.nl) must be notified immediately. The centre may request the service provider to suspend the services with immediate effect.

☐ BZ must be given the opportunity to perform an independent penetration test (no more than twice a year) on the services provided. Any low risks detected (CVSS <3.9) must be resolved within one month. Medium risks (CVSS 4.0-6.9) must be resolved within a week and high/critical risks (CVSS >7.0) within 24 hours. If this is not possible, the Information Security Centre (i-SecurityCentre@minbuza.nl) must be notified immediately.

D. Data encryption

☐ Authentication information must be encrypted at all times during transport and storage. Where necessary, encryption should be used for data transport and storage (including at rest).

[*] The backups must offer proven recovery options within the framework set by BZ (RTO, RPO, etc.).

[†] This must be carried out using production data at least once a year and in any case before going live.

☐ Only secure encryption technologies and methods may be used. These in any case include those recommended in the NCSC-NL TLS guidelines. Only the technologies categorised as 'good' in these guidelines may be applied. The latest NIST or CIS standards/frameworks also apply.

☐ Web applications must NOT enable http only, SSL 2.0, SSL 3.0 and TLS 1.0 traffic. However, web applications should enable TLS 1.2 connections or higher.

☐ Certificates[‡] must be deemed secure by the most common browsers[§] (in any case Internet Explorer, Edge, Chrome, Firefox, Safari).

☐ The certificates of the websites covered by the services must obtain a score of A or A+ in the ssllabs.com SSL server test.

E. Multi-factor authentication

☐ All accounts that can be used to access systems containing BZ data via the open internet must be equipped with two-factor authentication.

☐ All administrator and other accounts with high-level privileges for systems with access to BZ information must be equipped with two-factor authentication and these management interfaces must not be directly accessible via the internet.

F. Access control

☐ An access control matrix must be drawn up, maintained and applied for all access to data and systems that are used for the purposes of the Contract.

G. Physical security

☐ Physical access to systems and/or data must only be granted to authorised staff who have passed the correct background checks and have signed the correct confidentiality agreements.

☐ Appropriate security measures must be in place at locations where large amounts of sensitive data are processed, so as to prevent unauthorised access by means, for example, of piggybacking and social engineering.

☐ At these locations, authorised staff[**] must always wear a clearly visible access pass that clearly shows that they are authorised.

H. Communication security

☐ Sensitive data or large amounts of data must not be sent by email, unless the data is attached in a correctly encrypted container.

☐ There must be a data sanitisation procedure in place for information systems on which BZ information is or was stored. Due care should be taken to remove any residual data from these systems, preferably on the basis of NIST Special Publication 800-88, Guidelines for Media Sanitization. This also applies to systems for failover, mirrors, backup media and flash memory.

I. Data transfer

☐ The service provider must not grant parties other than those covered by this agreement (subprocessors and subcontractors) access to data or systems containing BZ data, unless explicit written permission has been obtained from BZ. In the bid document the service provider must have clearly stated which subprocessors and/or subcontractors are involved in the service provision.

[‡] Certificate types: Organisation Validation (OV), (preferred) Extended Validation (EV) and Qualified Website Authentication Certificate (QWAC).

[§] Internet Explorer (IE) 11 support ends on 15/6/2022, Microsoft Edge Legacy on 9/3/2021 and Safari on 1/10/2018.

[**] The service provider must have a physical access policy in place that sets out the requirement to wear the access pass in areas where customer systems are running.

☐ If the service provider is permitted to transfer the data in question to third parties, the service provider must lay down all requirements including the requirements in this information security schedule and the privacy requirements in the Data Processing Agreement in formally accepted contractual agreements with these third parties. The first service provider remains responsible and liable for proper compliance with the performance of the contractual agreements. It should also ensure that the provider continues to comply during the term of the agreement.

J. Security incident management

☐ Any information security incident, data breach or suspected incident related to confidentiality, integrity or availability must be reported without undue delay and in any case within 24 hours to the Information Security Centre (i-SecurityCentre@minbuza.nl). Any subsequent BZ instructions in response to this incident must be followed up immediately.

K. Business continuity and disaster recovery

☐ The contractor will take all reasonable measures[††] to ensure the integrity and availability of the data.

☐ In any case, this means that the contractor will ensure that data remains available in the event of failure or loss of the hosting location. The contractor itself decides which measures are appropriate as regards implementation, for example an encrypted backup set at another location or failover. The current backup policy must be complied with in this regard.

L. Logging and monitoring

☐ Logging: All access (including deleting and editing) to the data and systems that are used to fulfil this Contract is logged and processed in a centralised logging system for a period of at least 6 months.

☐ These logs contain the following (at a minimum): origin and destination IP address, usernames if possible, date, time, and actions taken.

☐ As part of the service, the contractor must actively monitor the environment and address any suspicious activity. BZ will be provided with a monthly report on security incidents.

☐ As part of the service, the contractor must ensure that systems and data are protected against viruses, malware and all other similar threats.

M. Audits

☐ The contractor must be able to demonstrate that it complies with ISO:27001/2, supported by an SOC 2 report or ISAE 3402 type 2 report.

☐ BZ must be given the opportunity at least annually to perform an audit or have an audit performed on all requirements as listed in this Contract.

☐ In addition to the above, during or after information security incidents BZ must be given the opportunity to conduct audits on compliance with the requirements specified in this Contract. The contractor must cooperate with BZ fully and in a timely manner.

☐ Audit findings showing non-compliance with the information security requirements specified in this Contract must be remedied immediately or within a timeframe agreed with BZ.

N. Non-compliance

☐ Failure to comply with the requirements of this Contract and/or this schedule may result in termination of this Contract, penalties and/or criminal prosecution

[††] The margin of reasonableness will be established in a programme of requirements and is dependent on other requirements.

Schedule 3: Agreements regarding Personal Data Breaches

Reporting a new/suspected breach

Under the General Data Protection Regulation (GDPR) the Ministry of Foreign Affairs (BZ) must notify the Data Protection Authority (AP) of data breaches **within 72 hours**. If all the details are not yet known, or if BZ is unsure whether an incident constitutes a data breach, a preliminary reporting form can be submitted. It is vital that, when faced with a data breach, Processors/subprocessors notify BZ's Information Security Centre **within 24 hours**, using this form, with a cc to the contracting authority's contact person.

Please note: This also applies to **suspected data breaches**.

The BZ Information Security Centre can be reached at **i-SecurityCentre@minbuza.nl**.

Once the form has been received, the Information Security Centre will carry out an analysis to determine whether the incident constitutes a data breach and will, where necessary, contact the Processor/subprocessor. This means that the reporting form will not automatically be forwarded to the Data Protection Authority.

Important: You should complete all fields, even if you do not know the answer in each case. Select the best choice and provide an explanation at the bottom of the form. For reporting to the Data Protection Authority, many of these fields are mandatory, which is why we ask you to always answer all questions.

1. Data breach reporting form for Processors/subprocessors

IMPORTANT: These fields are mandatory. Even if no correct answer is available as yet, try to answer the question as accurately as possible.

1.1 Who is reporting the data breach and is the contact person?

Name

Job title

Email address

Telephone number

Organisation

1.2 Involvement of another organisation

Was there another organisation (subprocessor) involved in the data breach?

Kies er een ▾

Name of the other organisation that was involved in the breach

In what way was the other organisation involved in the breach?

1.3 Timeline

Exact date on which the data breach occurred (if known)

Start date of the period during which the breach occurred

End date of the period during which the breach occurred

Is the breach still continuing at this time?

Kies er een ▾

When was the breach discovered?

If you are reporting the breach more than 24 hours after it occurred, please explain why.

1.3 Details of the data breach

1.3.1 *Nature of the data breach*

Breach of confidentiality of the data

Kies er een

Breach of the integrity of the data

Kies er een

Breach of the availability of the data

Kies er een

What is the nature of the incident that involved a breach of Personal Data?

Apparaat, gegevensdrager (bijv. USB-stick) en/of papier met persoonsgegevens kwijtgeraakt of gestolen

Provide a summary of the incident that involved a breach of Personal Data

1.4 Personal Data involved in the data breach

1.4.1 General Personal Data

Name

Kies er een

Sex or gender, date of birth and/or age

Kies er een

Citizen service number (BSN)

Kies er een

Contact details

Kies er een

Access or identification data

Kies er een

Financial data

Kies er een

Passports or other identification documents or copies thereof

Kies er een

Location data

Kies er een

Personal Data relating to criminal convictions and offences or related security measures

Kies er een

Unknown/other (please specify)

1.4.2 Special categories of Personal Data

Personal Data revealing a person's racial or ethnic origin

Kies er een

Personal Data revealing a person's political opinions

Kies er een

Personal Data revealing a person's religious or philosophical beliefs

Kies er een

Personal Data revealing a person's trade union membership

Kies er een

Data relating to a person's sexual behaviour or sexual orientation

Kies er een

Data relating to a person's health

Nee

Genetic data

Kies er een

Biometric data

Kies er een

1.4.3 Amount of Personal Data

Indicate (approximately if necessary) how many data records ('data registers') were affected by the breach

1.5 The group of people whose Personal Data is involved in the data breach

Staff

Kies er een

Customers (current and potential)

Kies er een

School pupils or students

Kies er een

Patients

Kies er een

Minors

Kies er een

Persons from vulnerable groups

Kies er een

Describe the group of people whose Personal Data is involved in the data breach

At a minimum, how many individuals' Personal Data is affected by the breach?

At a maximum, how many individuals' Personal Data is affected by the breach?

1.6 **Measures taken before the data breach occurred**

When the data breach occurred was the Personal Data encrypted or hashed or rendered incomprehensible or inaccessible for unauthorised persons in another way?

Kies er een ▼

If some of the Personal Data was incomprehensible or inaccessible, please specify which data.

If some of the Personal Data had been rendered incomprehensible or inaccessible, how was this achieved?

1.7 Impact of the data breach

1.7.1 Impact of the data breach on the confidentiality, integrity and/or availability of the data

Unauthorised persons could have been able to view the data

Kies er een ▼

The data could be misused in an improper or unlawful manner

Kies er een ▼

Incorrect, incomplete or outdated Personal Data may be being used within your own organisation

Kies er een ▼

Inaccurate, incomplete or outdated Personal Data could be reused for other purposes or passed on to other organisations

Kies er een ▼

An essential service provided to Data Subjects may have to be temporarily suspended

Kies er een ▼

An essential service provided to Data Subjects may have to be permanently discontinued

Kies er een ▼

Other (please specify)

1.7.2 Physical, pecuniary and non-pecuniary damage for Data Subjects

What impact could the data breach have on the Data Subjects' personal lives?

Discrimination

Kies er een ▼

Identity theft or fraud

Kies er een ▼

Financial losses

Kies er een ▼

Damage to reputation

Kies er een ▼

Loss of confidentiality of Personal Data protected by a duty of confidentiality

Kies er een ▼

Unauthorised reversal of pseudonymisation

Kies er een ▼

Data Subjects are prevented from exercising their rights and freedoms

Kies er een ▼

Data Subjects are prevented from exercising control over their Personal Data

Kies er een ▼

Other impacts (please specify)

Provide an estimation of the severity of the potential impact on Data Subjects

Kies er een ▼

1.8 Follow-up action in response to the data breach

1.8.1 Measures in response to the data breach

What technical and organisational measures has your organisation taken in response to the data breach and to prevent further breaches in the future?

1.8.2 Notifying parties

Have you notified Data Subjects and/or other parties?

1.8.3 International aspects

In which countries did the data breach occur?

1.8.4 Other information which could be useful

Where possible, please provide us with information that is or could be important for any follow-up investigation and which was not asked for or for which there was insufficient space to answer in the previous questions.

If a data breach has been identified, send this form to i-SecurityCentre@minbuza.nl, with a cc to the contracting authority’s contact person. Important: Always do this as soon as possible, but never more than 24 hours after discovering a data breach.