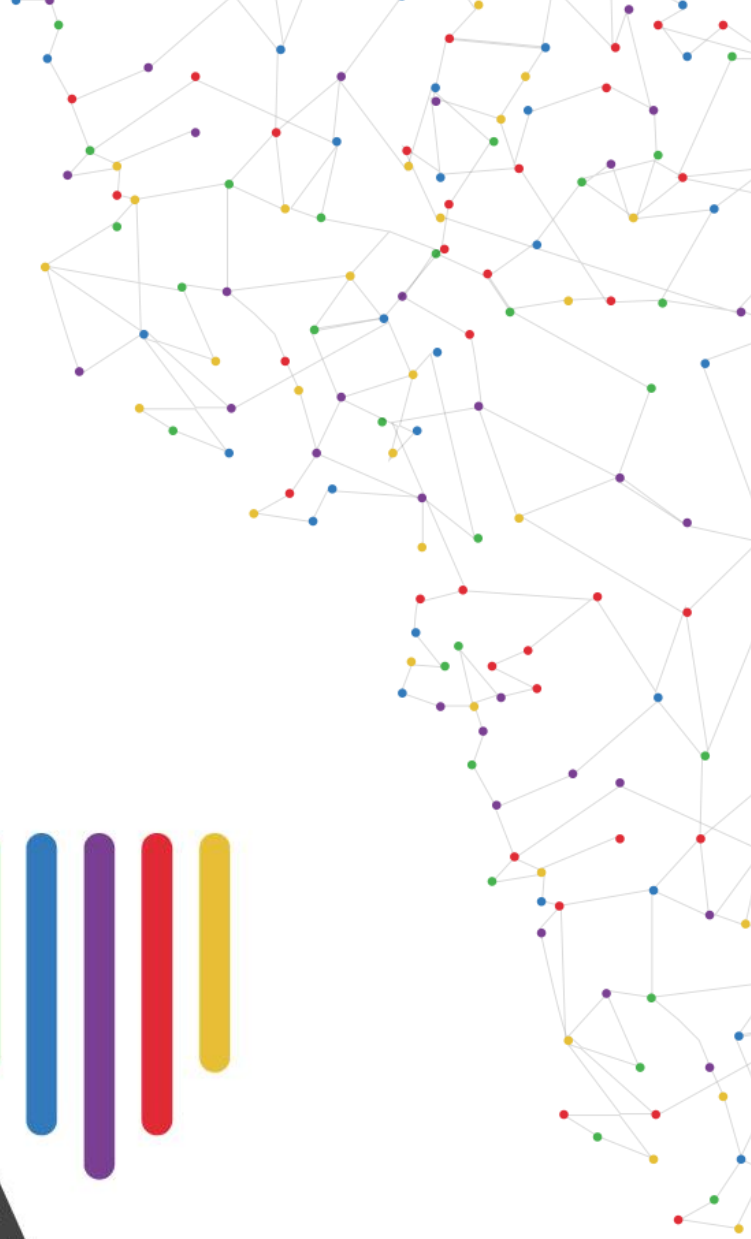

DATA PRO CREATED BY NEDERLAND ICT

DATA PRO CODE

Version: January 2018

For the digital economy

NEDERLAND ICT

THE CODE AT A GLANCE

Eight principles for professional data protection.

Specifically implementing current privacy and security rules.

Intended for small and medium-sized data processors.

CONTENTS

FOREWORD

The ICT sector is highly diverse, but one thing that most ICT businesses have in common is that they collect, process and store data at their customers' request. There are statutory guidelines with respect to privacy and security for organisations serving in this role of 'data processor', particularly the new European Data Protection Regulation (GDPR). Nederland ICT has developed the Data Pro Code to help businesses comply with those rules.

For data processors, the Data Pro Code is an instrument for treating data in a secure and privacy-friendly manner. The eight principles in the code represent a concrete implementation of current legislation. The code offers ICT businesses a framework and guidance for processing data and ensures openness and accountability towards their customers.

Nederland ICT has developed the code jointly with its members. In developing the code, we explicitly based ourselves on the practice of small to medium-sized ICT businesses. It should be feasible for any ICT business, however small or large, to apply the code.

By applying the Data Pro Code, data processors demonstrate that they subscribe to treating the personal data entrusted to them in a professional manner. For customers and partners in the chain, the code offers clarification and transparency on what they are entitled to expect from ICT businesses.

Accordingly, I am confident that the Data Pro Code provides a solid basis for the further professionalisation of the sector and for mutual confidence in the market.

Lotte de Bruijn, Director Nederland ICT

STARTING POINT

With the Data Pro Code, Nederland ICT is taking on its responsibility as industry association for the ICT sector

The European privacy rules (GDPR) outline general principles for treating personal data. As the interpretation and implementation of those principles differ widely between sectors and even, in fact, between businesses in practice, the GDPR expressly refers to the role of industry associations in implementing the GDPR.

By developing the Data Pro Code, Nederland ICT is stepping up to fulfil this role. We are also shouldering our responsibility to further professionalise the sector with regard to privacy and security. The Data Pro Code is aimed at promoting clarity and transparency in the market and hence increasing confidence in the ICT sector.

The Data Pro Code is for data processors

Businesses that collect, process and store data for their clients are 'data processors' under the GDPR. The Data Pro Code has been developed on the basis of that legal role. By applying the code, a business fulfils its role as a data processor in a professional manner. The term Data Pro references those twinned legal (data processor) and commercial (data professional) aspects of privacy.

The Data Pro Code specifically implements the GDPR

By applying this code, data professionals can signal to the outside world that they:

- have thought about how to deal with personal data;
- have organized their organisation to safeguard the secure treatment of clients' personal data.

This code therefore represents a practical, specific implementation of the requirements set out for data processors in the GDPR.

The Data Pro Code is based on voluntary, normative principles and best practices

The Data Pro Code does not absolve organisations from their own responsibility. The code provides a normative framework for the protection of personal data ('data protection') for data processors. The Data Pro Code accordingly presents general principles. The principles in the code are translated into practice-based recommendations, i.e. 'best practices'. These can be read in a variety of ways: 'this is how it's done' or 'these are good practical examples.'

Anyone wishing to depart from the code, owing to the nature or size of his organisation, is free to do so. But it is important, given the manifest need for accountability and transparency, to explain this whenever that is the case. Hence the principle 'comply or explain' applies.

The Data Pro Code is for all data professionals, from micro to large

The basic premise in developing the code was the practice of small and micro organisations as referred to in the GDPR. Small organisations are organisations with fewer than 50 employees, while micro organisations have fewer than 10 employees. This does not mean that the code is not applicable to larger organisations. Any service provider, however large or small, that considers itself to be a data professional can apply the Data Pro Code.

The Data Pro Code offers clarity and transparency

The organisations that adhere to this Data Pro Code inform their clients how they have safeguarded data protection in their organisation. They also provide information on what their services or products are suited to, with regard to an assessment of personal data protection. That enables clients, whether they are controllers or data processors, to assess for themselves whether and how they wish to use the products and/or services of an organisation that processes personal data for them. Applying the Data Pro Code means that you document and explain the measures you have taken to protect personal data.

Dutch and English version

The Data Pro Code was originally drafted in Dutch. The English version is for convenience only. IN case of conflict between the Dutch and the English version, the Dutch version prevails.

THE DATA PRO CODE

PRINCIPLE 1 - DESCRIPTION AND ASSESSMENT OF SERVICE PROVIDED

The services or products offered by the data processor are described and assessed by the data processor, taking into account the market in which it operates, the intended use by the data processor of its service or product and therefore the expected nature of the data to be processed in or with its service or product and the number of data subjects to be processed.

1. The data processor has provided a clear description of the intended use of its service or product.
2. The data processor has described the expected nature of the personal data to be processed in or with its service or product (yes/no special categories of personal data?).
3. The data processor has assessed the market in which it operates and has adapted its service or products to that assessment *(privacy by design*), taking into account :
    - the number of data elements per data subject (*data minimisation*);
    - the expected number of data subjects to be processed (more than 100,000 data subjects?);
    - the intended use of its service or product (its service or product is/is not crucial to the client's business operations?; *Data Protection Impact Assessment (DPIA) on the services*).

PRINCIPLE 2 - POLICY AND GOVERNANCE

The data processor has a documented policy for data protection, including a procedure for data breaches.

1. The data processor has documented its choice of the level of the security measures to be taken by it (*vision and mission for data protection*).
2. In designing its own service or product, the data processor has taken measures to avoid processing of non-necessary personal data in the use of its service or product (*privacy by design*).
3. The data processor knows what to do in case of a data breach (*data breach protocol*).
4. The data processor has designated a contact person who possesses (or acquires through training) knowledge of data protection.

PRINCIPLE 3 - ORGANISATION AND MEANS

The data processor has identified and listed its data processing operations.

1. The data processor has identified and listed the means it deploys and the suppliers it uses (*there is an overview of means and suppliers ((sub)data processors) that are required for its service provision*).
2. The data processor has assessed whether the means it deploys and the suppliers ((sub)data processors) it uses provide adequate safeguards concerning data protection.
3. The data processor has accurate contract records (*and can thus comply with the obligation to maintain records regarding processing activities*).

PRINCIPLE 4 - RESTRICTIONS ON USE

The data processor has safeguards in place ensuring that the personal data obtained from its client are used solely for providing its services to that client.

1. Personal data of a client are separated by the data processor from personal data of other clients.
2. Staff of the data processor are obliged to treat confidentially the personal data of a client.
3. After the end of the agreement with the client, the data processor can provide personal data to the client in a machine-readable format if this has been agreed.
4. The data processor safeguards that after the end of the agreement with that client or after the completion of an assignment for that client, personal data of the client will within three months of the end thereof be removed in such a way that they can no longer be used and are no longer accessible (*render inaccessible*);

PRINCIPLE 5 - PROTECTION OF PERSONAL DATA

5.1 The data processor has implemented appropriate technical and organisational measures to safeguard a level of security for personal data that is appropriate to the risk associated with the use intended by the data processor of its service or product.

1. The data processor can adhere or conform to a security standard or checklist recognised in the sector.
2. Data processor shall choose his own list of security measures specifically tailored to its product or service.
3. In choosing the security measures, the data processor took account of the following security measures:

    - pseudonymisation and encryption of personal data;

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability of and access to personal data in a timely manner in the event of an incident (back-ups, redundancy).

5.2 In assessing the appropriate level of security the data processor shall take into account the risks presented by processing that are associated with its service or product, in particular from accidental or unlawful destruction, loss, alteration, unauthorised access to personal data within or via its service or product.

1. In assessing an appropriate level of security, the data processor shall take into account:
   - the state of the art;
   - the costs of implementation;
   - the probability, likelihood and severity of the risks for the rights and freedoms of individual data subjects;
   - the market in which it operates;
   - the number of data elements and the expected nature of the data to be processed (yes/no special categories personal data?);
   - the expected number of data subjects to be processed (more than 100,000 data subjects?);
   - the intended use of its service or product by a client (its service or product is/is not crucial to a client's business operations?).

5.3 The data processor applies an information security management system or security standard, providing for a process for regularly testing, assessing and evaluating the effectiveness of the security measures for personal data taken by the data processor (*plan, do, check, act*).

1. The information security management system or security standard chosen by the data processor is documented in its data protection policy.
2. The data processor can adhere or conform to one or more security standards recognised in the sector.

PRINCIPLE 6 - OBLIGATION TO PROVIDE INFORMATION – DATA PRO STATEMENT

6.1 The data processor shall inform its client of the security measures taken regarding its service or product in such a way that a client is able to assess whether these are adequate in view of the use of the service or product intended by the client and associated possible processing of personal data (*Data Pro Statement*).

1. The data processor has published a 'Data Pro Statement' or it is included in the data processing agreement.
2. The Data Pro Statement shall as a minimum include:
    - the information security management system, the security standard(s) chosen by the data processor;
    - if applicable, the certification(s) of the data processor;
    - whether the data processor processes personal data, or has personal data processed, outside the European Economic Area (EEA);
    - whether and which (sub)data processors are used by the data processor;
    - the period during which data are retained, if it departs from the 3-month time limit for destruction in 4.4;
    - the contact details of the contact person for data protection within the organisation of the data processor.
3. In the Data Pro Statement, the data processor shall provide information on the following security measures as a minimum:
    - pseudonymisation and encryption of personal data;
    - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    - the ability to restore the availability and access to personal data in a timely manner in the event of an incident (back-ups, redundancy).

6.2 In principle, the data processor will use the Standard clauses for processing pertaining to the Data Pro Code in its data processing agreement.

1. The data processor shall note in its contract records whether the Standard clauses for processing apply.

6.3 If the data processor discovers a data breach in its organisation, the data processor shall inform its client thereof as soon as possible in order that the controller can comply with its statutory obligation to notify the Dutch Data Protection Authority or the data subjects concerned thereof within 72 hours after having become aware of it. Whether or not to provide such notification remains the responsibility of the controller.

1. If required, the data processor shall support the client or the controller in the notification process.
2. In the event of a data breach, the data processor shall provide the required information, and as a minimum:
    - a description of the incident, nature of the data breach, nature of the personal data and categories of data subjects concerned, an estimate of the number of

data subjects concerned and databases potentially involved, an indication of when the incident took place (*what happened?*);

- contact details of contact person (*whom can the controller contact with questions?*);
- possible consequences (*what can happen, what does the controller or the data subject need to beware of, point out the possibilities for identity fraud if details such as BSN (citizen's service) numbers, login and password details, copies of passports may have fallen into the wrong hands*);
- measures taken (*what has the data processor done to limit potential damage or prevent it in the future?*);
- measures to be taken by the controller or data subjects concerned (*what can the data subjects concerned do themselves, for instance 'monitor e-mail, change passwords');*
- the data processor shall continue to update the client on further developments.

PRINCIPLE 7 - RIGHTS OF DATA SUBJECTS

The data processor shall inform its client whether it has established processes and procedures by means of which a client who is a controller can comply with the rights of data subjects.

1. The data processor shall inform its client of the possibilities for data subjects to exercise their rights, including the right of access, rectification, objection and the right to be forgotten, in relation to the service provided by the data processor to its client, for instance in the Data Pro Statement.

PRINCIPLE 8 - ACCOUNTABILITY

The data processor shall regularly test and evaluate its data protection policy and security measures taken and shall modify these if required.

1. The data processor applying the Data Pro Code can have itself tested independently. If the result is satisfactory, the data processor can use the Data Pro Certificate, with which it can demonstrate its compliance with the Data Pro Code.
2. The certified data processor will be included in a publicly accessible register.
3. The certified data processor can be tested during a year (on a sample basis or following complaints) and will re-test or have itself re-tested annually.
4. The right to use the Data Pro Certificate can be revoked by the certifying body following complaints or following an investigation. The data processor's right to use the certificate shall lapse following an unsatisfactory result in the event of re-testing.

5. The data processor shall periodically inform its client about the (internal) reviews performed by it, for instance by:
   - recertification obtained or not obtained, for instance by a reference to the publicly accessible register;
   - information about periodic external reviews such as audits or by providing a Third Party Memorandum (TPMs);
   - information, or relevant sections from, an assurance report with conclusions concerning the auditor's findings;
   - own reviews or own statements by the data processor.
6. The data processor will implement the recommended improvement measures following a review insofar as it can reasonably be expected to do so.

GLOSSARY

	Defined in the Dutch text of the GDPR as:	
Controller	*'verwerkingsverantwoordelijke'*	In accordance with GDPR: *'a 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'.*
Data processor	*'verwerker'*	In accordance with GDPR: *'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'*
Data protection	*'gegevensbescherming'*	Protection of personal data.
Data subject	*'betrokkene'*	In accordance with GDPR: *'an identified or identifiable natural person'.*
Client		The client can be both a controller or another data processor engaging the data processor to process personal data.
Personal data	*'persoonsgegevens'*	In accordance with GDPR*: 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.*
Standard clauses	'standard contractual clauses'	The standard contractual provisions as referred to in article 28 (8) of the GDPR.
Processing	*'verwerking'*	In accordance with GDPR: *'operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.*

Data processing agreement		The contract that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller; as described in article 28 (3) of the GDPR.