Specialisterren Data Protection Policy

Date:	2018-06-07
Version:	1.0
Author:	Specialisterren
File Name:	GDPR_DPP_20180607.doc

Specialisterren Data Protection Policy

Introduction

Specialisterren is a specialised organisation that performs testing for third parties. As such it has little third party data and is not expressly a data processor of its own data or data from third parties. It does have some personnel data, including employee and customer data.
As a testing organisation it has access to tests systems and data of its clients. It is the intention that all test data is anonymous and thus expressly is *not* PII. However allowance has to be made for issues in the anonymisation processes when test data could contain personal information.
The topics below further explain Specialisterren's policy to handling data in general and personnel data in particular.

GDPR Topics

The Data Protection Policy will comply with the GDPR and specifically with the topics indicated in that regulation as follows:

Awareness

Specialisterren will define and implement an Awareness Programme that will have the following purposes:

- Ensure that all employees are aware of the GDPR and what it means, as well as be aware of their rights and responsibilities with respect to the GDPR;
- Ensure that all employees are able to recognise potential personally identifiable Information (PII) should this occur when testing or during other activities;
- Be aware of the internal process that is to be used should suspected PII be seen;
- Be aware of the responsibilities related to storing (test) data and potential PII data on systems not owned by the organisation (i.e. making copies on laptops or USB sticks etc. in order to test the testing procedures);
- Ensure that all employees authorised to work with internal data (employee, customer etc.) are aware of their responsibilities with respect to working with this data;
- Ensure that all new employees are made aware of the awareness process and likewise ensure that employees who leave Specialisterren do so without taking any PII data with them;
- Ensure that all employees are made aware of the need to refresh their awareness of the Data Protection Policy within Specialisterren and ensure that they actively follow this policy;
- Be able to show the awareness process and all associated material, along with all records of attendance etc. to any authorised party such as an auditor etc.
- Ensure that the awareness process is initially and thereafter, at a regular interval, reviewed to ensure that it is compliant with the GDPR and this policy, is adequate to reflect the business needs of Specialisterren and also reflects the experience built up within the organisation;

Data Register

- Specialisterren will maintain an active record ("Data Register") of all PII that it actively holds and processes;

- The Data Register will be regularly reviewed to ensure that it is actual and up-to-date.
- Any changes in legislation and / or experience with handling PII will be used to review the Data Register;
- All changes to the Data Register along with who made the changes, and who approved them will be kept for audit purposes;

Communication

- The Awareness Programme will be one of the most important mechanisms to communicate the GDPR policy to its employees;
- Specialisterren will ensure that all data subjects know what their rights are with respect to their PII and will know how to exercise their rights;
- Specialisterren will clearly indicate for how long it needs to keep PII and why;
- The Awareness Programme will be available within the organisation to all its employees, customer and other relevant data subjects. It will also be clearly documented and available for audit purposes etc.;
- Specialisterren processes very little data but recognises the rights of those data subjects. Specialisterren will ensure that these rights are made available to data subjects and will have adequate processes in place to ensure that they can be exercised;
- In order to handle the undesirable situation when test data contains data that could be considered PII, and thus is subject to rights of the data subjects, internal processes and agreements with customers will be provided and used.

Request to access

- Specialisterren recognises that data subjects have the right to request access to their data, along with the rights to manage (delete, move and modify, where applicable) their own data;
- Specialisterren will make available within the organisation and in a suitable manner to customers and other data subjects, processes to ensure that data held by Specialisterren.

Legal basis for processing personnel data

- Specialisterren understands and recognises that there needs to be a legal basis for the use the of all PII;
- Specialisterren will document the legal basis for processing PII and will make this information available within the organisation as well as to customers and other data subjects;
- A regular, documented review of the legal basis will take place to ensure that this information is kept up to data and reflects current regulation;

Permission

- Specialisterren understands that permission is required for PII to be used and that it is required that Specialisterren clearly specifies why it needs certain PII;
- As needed existing contracts (customers, employees etc.) will be reviewed to

ensure that this information is provided and also to ensure that the data subject understands what permissions he is providing and why;

- If additional information is required from a data subject and / or this information must be supplied to third parties, then this will be explained to data subjects and additional permissions expressly requested;

Handling data of non-adults

- Specialisterren has no business with processing non-adult data and will expressly forbid the handling of this data within the organisation;
- Should PII of non-adults be found within test-data, then this will be reported to the relevant client and measures taken as appropriate;
- These procedures will be clearly documented and also agreed with (potential) customers. These procedures will form part of the contract with the client;

Data leaks

- Specialisterren has a general policy of only storing as little PII data as is necessary. However Specialisterren recognises that even when the best care is taken with data, faults and thus data leaks can occur;
- Specialisterren will provide and use simple, clearly defined procedures that will be carried out when any data breach is detected;
- Specialisterren will also actively carry out activities to ensure that any data breach can be detected in a timely manner and thus can lead to the activation of the data breach processes;
- Specialisterren will make use of active protection (that is encryption with good password management) when possible rather than rely on ad-hoc data leak detection.
- Specialisterren will co-operate with its customers and its data centre providers and other suppliers to ensure that any data breach procedure is, as far as possible seamless and is able to meet all regulatory requirements;
- All use of data breach procedures (along with tests of these procedures) will be recorded for audit purposes along with the results;
- The data breach procedures will be regularly reviewed to reflect experience gained with data breaches (either actual or tests) and with regulatory changes;
- All review processes will be recorded;
- All data breach processes and all information pertaining to them (such as tests, revisions etc.) will be available to auditors, regulatory bodies etc. as required;

Privacy by design

- Specialisterren main business function is to provide test facilities for other organisations. Therefore there is no implicit design taking place. However some test tooling is deployed and enhanced and thus Specialisterren employees must be aware that use of PII and privacy in particular must be considered;
- Privacy by design will be handled in the Awareness Programme and will be subject to the review process.

Specific role for data protection

- Specialisterren recognises the need to implement this Data Protection Policy correctly and in a provable manner within the organisation. Therefore all programmes and processes as defined are to be implemented using processes that show that have been considered and implemented in a deliberate and prove-able manner;
- Specialisterren, based on its current business does not need to formally define a Data Controller . However Specialisterren will define certain clearly defined roles and functions so that processes and programmes are then operated under the auspices of this role.

International rights

Specialisterren operates within the Netherlands and therefore will operate with the Netherlands authorities. https://autoriteitpersoonsgegevens.nl/