HICT

Data Protection Policy

OPTIMISING HEALTHCARE

[Updated: 23/12/2019]

The importance of data protection

Hict attaches great importance to the correct protection of the data it processes, in particular personal data. Through this policy, Hict wants to establish at a strategic level how data is protected, what responsibilities have been assigned to it and what priorities Hict has determined with regard to data protection.

In particular, Hict wants to protect the data of customers and the personal data they provide against:

- Loss: data is no longer available
- Leaks: data ends up in the wrong hands
- Errors: data is incorrect, for example outdated or incomplete
- Not accessible: data is not accessible at the time of care
- Unauthorized viewing: viewed by persons who are not authorized to do so
- Not being able to find out who viewed, changed or deleted the data
- Processes that are not in line with regulations, guidelines and standards

In this policy, the management wants to appeal to everyone involved in electronic and paper processing in order to ensure that the processing of personal data takes place correctly, based on a common vision and our joint desire to offer quality services.

This policy manual looks in more detail at the protection of the privacy of, and more specifically, informational, privacy. This policy manual serves as a standard for the processing of personal data of customers and their insured by Hict . It is a guideline for all processing processes and offers a reference standard for audit and control. The policy handbook offers every stakeholder, employee or involved external person an insight into the data protection policy and the way in which we handle sensitive personal data.

The manual is also written for anyone who has a function within Hict where personal data is processed. They use (parts of) this policy handbook to design procedures and guidelines for employees and external parties, such as IT suppliers. The relevant parts of this policy manual are processed in agreements with staff and suppliers.

The organization of data protection

Competence

As the controller, the authority of this policy lies with Hict , represented by its director. The director is responsible for formulating and determining, and supervising, compliance with the policy principles within Hict , supported here by the Executive Committee / management team / etc ..

Responsible implementer

The executive committee acts as a formal decision-making platform for data protection. The executive committee is authorized to take decisions concerning the following aspects:

- The risk analysis and associated methodology;
- Developing the data protection policy and the accompanying guidelines;
- The implementation of security measures (ie the content of the security plan)
- The structural response to data protection problems and advice (within 3 months);

The DPO

The substantive follow-up of the data protection policy lies with the Data Protection Officer (DPO). He / she performs this task according to the provisions in the GDPR.[1] Hict passes on the identity (and any changes) of the DPO to the data protection authority. The DPO reports to the director of Hict and is in particular charged with:

- Submit recommendations and recommendations to the executive committee
- Promote the awareness of all actors within Hict
- Supervises compliance with data protection policy within Hict
- Documents what is needed with regard to data protection, such as a safety plan and the processing register
- Performs the specific tasks assigned to the DPO under the GDPR[2]
- Registers violations and submits these, together with an advice, to the management committee.

The employee

Anyone (internal or external) who processes data (for example, view, register, change, etc.), does this according to the policy principles in this policy manual. The user processes data in accordance with the duty of discretion and in accordance with the following principles:

- Is responsible for the data of data subjects that he / she processes
- Carries out the safety guidelines during his / her processing order.
- Only processes the data that belongs to the task
- Is responsible for the data
- Reports breaches
- Complies with article 458 of the Criminal Code: The user respects professional secrecy.

IT employee or key user

In addition to the user's responsibilities, the IT employee or key user is responsible for:

- The implementation of the technical measures
- Implement the safety settings in line with this policy manual.
- Report the safety problems that arise before, during or after the implementation of IT resources to the DPO
- To act as an expert. From this role he / she participates in the identification as well as in the remediation of the data protection risks
- Comply with the code of conduct.

IT supplier

The IT supplier has the same responsibilities as those of an IT employee. Additional:

- He points out the safety risks of delivered applications
- The supplier points out the safety tasks to be included
- Does the supplier pursue a transparent data protection policy by communicating about its own current security level and when dealing with security incidents.

[1] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
[2] Article 39 of the GDPR

Scope of the data protection policy

This policy applies for the entire life of information within Hict , from obtaining information to the eventual removal of information within the organization.

This policy applies to whole Hict:

- Hict 's office
- All staff members of Hict , both internal employees and externals who are employed within Hict for a fixed or indefinite period.
- All assets and information processing systems managed by Hict as well as systems managed by external parties for the purpose of information processing for Hict such as databases, information regardless of its carrier, networks, data centers, etc.
- All processing activities, both as a controller and processor.

For certain domains or processes within Hict , additional guidelines or procedures can be worked out that describe in detail what measures are being taken to achieve the desired level of data protection. This policy is the framework for all other guidelines or procedures.

In view of the important role of IT suppliers in setting up the IT environment to process data, the policy handbook also lays down the policy principles for this.

Risk management

Hict brings risks of data mapping on the basis of a risk analysis, which was first performed in the quarter of 2018 and repeated in the third quarter of 2019. The risk analysis based on the following criteria (ranking system):

- The guidelines regarding the information security of personal data, as published by the Commission for the Protection of Privacy
- The General Data Protection Regulation
- The ISO 27001 standard on information security

The analysis identified operational and tactical risks. These risks were discussed with the management on 16/09/2019. The findings from the risk analysis were discussed and are included in an action plan to deal with the risks found. In this, Hict recognizes four possible risk treatments:

- Accept: a risk is accepted, no additional measures are taken. Hict strives to accept as few risks as possible.
- Transfer: a risk is transferred so that the responsibility for the risk no longer rests with Hict .
- Restrict: Hict takes the necessary measures to limit a risk so that the risk is reduced to a level at which it can be accepted.
- Exclude: Hict takes measures to prevent a risk from occurring at all.

The aim is for the risk analysis to be reviewed at least annually. This is part of the DPO's work.

Policy objectives for data protection

Hict, both in its role as controller and processor:

- Is transparent about the personal data that it processes and the processing purpose, both to the data subject, the customers and the regulators. The communication is honest, easily accessible and understandable. The transparency principle also applies when the personal data are exchanged.
- Only processes the data that are relevant to the performance of its duties. Every task involving the processing of personal data is lawful . This means, among other things, that the processing is in accordance with the legal and statutory objectives of Hict . This is evaluated in each case when a new processing target, as necessary, on the basis of a gegevensbeschermi ng seffectbeoordeling .
- Only processes personal data that is strictly necessary is for the implementation of activities. In this way, identifiers associated with the personal data are reduced to a minimum.
- Supervises the integrity of the personal data during the entire processing cycle.
- Does not store data longer than necessary. The necessity has been tested against legal obligations and the rights and freedoms of the person concerned.
- Prevents breaches that result from the processing of personal data. Information security, data protection in design and privacy-friendly default settings are tools for this. When an infringement takes place, this is reported in line with the relevant regulations.
- Is able to execute all applicable rights of a data subject, such as the right to view, copy and possibly also delete. Hict hereby monitors any restrictions that apply to these rights.
- Actively ensures that when processing personal data for a specific purpose, the rights and freedoms (for example, the right to insurability, the right to care) of the person concerned remain protected.
- Processes data in line with the rights and freedoms that apply in the European Economic Area and checks its application when the data is exchanged outside it. Hict therefore complies with all legal and normative frameworks (ie both Flemish, Federal and European rules) when processing personal data and has therefore clearly mapped its responsibility for the personal data and that of others. Hict also monitors and applies the codes of conduct applicable in the sector.
- Is able to demonstrate compliance with all policy objectives, in accordance with legal provisions. This accountability is monitored by internal supervision and control and is enforceable in accordance with the legally applicable principles.

Priority action points from the risk analysis

Below are the various priority action points that emerged from the risk analysis. This concerns the findings with a score of High or Critical.