Working with personal data and confidential information in a secure manner

Title	Working with personal data and confidential information in a secure manner
Reference	ISMS.veilig_werken
Type	Guideline
Classification	General
Distribution	All staff and students (via portal, under Information Security)

Version	Date	Author(s)	Description and history
1.0	20.2.2015	Michel Raes	Draft for review, including ICT Committee on 27 February 2015
1.7	19.6.2015	Michel Raes	Proposal to ICT Committee on 26 June 2015
1.7b	29.6.2015	Michel Raes	Document approved by the Executive Board on 10 July 2015
1.7c	18.8.2015	Michel Raes	Document accepted by the negotiation committee for university staff (Dutch abbreviation POC) on 30 September 2015
1.7c_EN	1.12.2015	UCT / Michel Raes	(unofficial) English translation

Table of Contents

1. Objective of this document

This document sets out the policy for the secure handling of personal data and confidential information at Ghent University.

The policy works on the premise that personal data is processed securely in accordance with privacy laws. The guidelines in this regard, however, apply equally to the secure processing of other confidential information.

This follows on from the basic principle of a combined approach on privacy protection and cyber security, as defined in the vision of information security at Ghent University.

2. Scope

The present policy applies to all persons who, in their relationship with Ghent University, collect, generate, use or process personal data and other confidential information, both in electronic and non-electronic form.

The **persons concerned** may have different statuses.

- Staff who have a **statutory, or contractual, working relationship with Ghent University** (salaried employees) are held, on the basis of the relevant labour regulations and any additional codes of conduct, to their responsibilities involving the information they handle; in this case, information security.

- For **unpaid staff, students** or other persons who do **not have a contractual working relationship** with Ghent University, the responsibility for the information they handle (in this case, information security) must be regulated in specific agreements with nominative confidentiality clauses. For students, in particular, the wording of the responsibilities must be seen as forming part of the admission agreement concluded with Ghent University.

Where applicable, the same policy will apply to external staff and service providers, except that for them, a more specific policy is drawn up (in accordance with the three-year plan for information security 2015-2017).

3. Policy Statement

Ghent University commits to observing all applicable laws and regulations relating to the secure handling and protection of personal data.

Consequently, those who collect, save or process personal data in the course of their activities at Ghent University must take it **upon themselves** to observe the guidelines for the **secure processing of personal data**.

Prior to processing personal data, the staff and students of Ghent University must check which laws and regulations must be observed.

If applicable, they must meet the requirements for declaration to, or prior authorisation by, the Privacy Commission, and they must observe the conditions of the prior authorisation decision.

Staff and students at Ghent University are expected to consider **possible risks relating to information security**, to address those risks using common sense, and, where necessary, to take the initiative to ask for assistance; e.g. from their line management or Ghent University's information security counsellor.

By extension, the same also applies to **the secure handling of other confidential information** at Ghent University.

The present policy is linked to practical guidelines and other actions to provide support. In the first instance, reference is made to the IT resources and support offered centrally from the ICT Department at Ghent University.

In addition, appropriate measures will be taken to raise awareness and a sense of empowerment, and to communicate and disseminate this policy.

4. What are personal data and confidential information?

The document “Information Security - Guidelines for the classification of information and data” defines personal data, lists special categories of personal data, and details the difference between confidential and non-confidential (i.e. general) information. It also contains information about ownership and responsibilities when handling such information.

5. Working with personal data and confidential information in a secure manner

5.1. General: working with IT resources in a secure manner in practice

The extensive computerisation of activities at Ghent University creates vulnerabilities and dependencies that involve IT-related security risks.
That is why, as an integral part of this policy document, a number of more technical guidelines are offered to end users: **“10 points for working with IT resources in a secure manner in practice”** (see Addendum 1).

Moreover, system operators at the faculties and departments also have an important role to play in keeping IT services secure. The guidelines in the **“10 points for system administrators for securely managing servers and services”** (see Addendum 2) apply to them.

5.2. Working with personal data and confidential information in a secure manner in practice

Privacy legislation requires Ghent University to take technical and organizational measures to guarantee the secure processing of personal data.
Therefore, for the **secure processing of personal data** that involves IT resources at Ghent University, the **"10 pointers for working with IT resources in practice in a secure manner"** (Addendum 1) must be **strictly observed**. By extension, the same policy applies to working with other confidential information in a secure manner.

Most of the security requirements based on privacy legislation are met when the central infrastructure is used (e.g. central personal and shared disk space), and the platforms and applications that are provided centrally (e.g. via Athena).

Local storage and local processing of personal data on the staff's and students' own equipment is discouraged. Instead, it is advised to store data on the centrally available workspace hosted by the **Department of Information and Communication Technology (DICT)** - (the "H:disk").

If local copies of personal data do still occur, then these must be encrypted securely and reliably with cryptographic tools.

For encryption, specific guidelines and a number of best practice recommendations will be issued in due course. It is up to the users to familiarize themselves with the cryptographic techniques and tools used and to apply them correctly[1].

Elaborating on the practical aspects, Addendum 3, "Working with personal data and confidential information in practice in a secure manner" focuses on the secure handling of personal data on the central infrastructure in the context of prior authorisation by the Privacy Commission.

N.B. Non-digital personal data and confidential information should also be kept, processed and archived with due care and responsibility, and in accordance with the applicable laws and regulations.

6. Applications and examples

6.1. Research projects that make use of personal data

Researchers and students (e.g. Master's dissertation students) who work with personal data are expected to take note of this policy, the accompanying guidelines (particularly the guideline for the classification of information and data) and of the "Information for the researcher" guides from the Privacy Committee (only in Dutch):
http://www.privacycommission.be/nl/brochures-voor-de-onderzoeker

[1] Responsibility and liability of employees subject to a formal encryption policy becoming available (including instructions and support).

According to the Privacy Act, the "**processor**" is the natural or legal entity who determines the purpose of, and resources for, processing personal data. Accordingly, Ghent University is liable and ultimately responsible for the secure handling of personal data. Based on the principle of **empowerment,** however, this responsibility is shared with the **research coordinator** (see also the document "Classification guidelines for information and data").

Data management, or the sound, effective handling of research data, forms an essential part of the research process. When personal data is processed, privacy protection and secure handling are important issues in the management of data. If necessary, data management can be formalized by drawing up a **data management plan** (as is already required for some research funding). See
https://www.ugent.be/intranet/nl/onderzoek/beleid/datamanagement (in Dutch)
http://www.ugent.be/en/research/research-staff/organisation/datamanagement (in English)

Regarding information security, data management involves thinking about, and/or implementing:

- risk management (what are the data-related information security risks?);
- data minimization (only collect and/or process those personal data that are needed for the research goals);
- the anonymisation or pseudonimisation of personal data (often required; e.g., in the subsequent processing of previously collected information);
- a secure storage strategy (including setting the correct length of time for the information to be retained);
- a secure processing strategy (e.g. with centrally provided applications on the central infrastructure);
- a secure disposal strategy (after the expiry of the time set for the information to be retained).

Where necessary, the researcher will take the initiative on gaining additional information and advice about the aforementioned aspects of information security, e.g. from the information security counsellor at Ghent University.

6.2. Prior authorization for requesting personal data from external sources

To request personal data from external sources, special permission – an authorization – is often needed, from a sectorial committee of the Privacy Committee, or from the Flemish Supervisory Commission.

Authorization is to be requested from the Flemish Supervisory Commission when personal data from a Flemish public body is provided electronically.
See http://vtc.corve.be/machtiging_aanvragen.php (in Dutch)

The sectorial committees of the Privacy Committee may issue authorization in all other cases.
See https://www.privacycommission.be/nl/een-machtiging-aanvragen (in Dutch)

To protect privacy, it must be made clear in the application for authorization how the information is being handled securely, by completing a security document. Moreover, the information security counsellor is to be consulted about, or at least informed of, the dossier.

Ghent University is committed to regulating information security not only on paper and administratively, but also to bringing this to the fore as an important area of concern in practice.

If the guidelines of the present policy document are followed in practice, particularly the guidelines in Addendums 1, 2 and 3, then the lion's share of the security requirements for authorization will be met.

An important point is that there must always be a list of people who can access the relevant personal data. These people must, in accordance with present policy, honour their responsibilities in terms of the confidentiality and secure handling of personal data.

6.3. Administrative applications involving personal data

Ghent University staff who work with personal data in administrative applications are expected to take note of this policy and the relevant guidelines (particularly the guideline for the classification of information and data).

Similar to the situation involving research projects, Ghent University is liable, and ultimately responsible, for the secure handling of personal data, but based on the principle of empowerment, however, this responsibility is shared with the coordinator who is responsible for the administrative application.

For certain administrative applications, it may be useful to draw up additional policy documents or codes of conduct on privacy protection. For example, reference can be made to the existing "Code of Conduct for the use of the educational administration and student information system" and the "Good practices for handling requests concerning personal data (in the context of student administration)".
See http://www.UGent.be/intranet/nl/onderwijs/intern/oasis (in Dutch)

7. Exceptions and deviation from the policy

This policy and the accompanying guidelines come into effect on the date of their approval by the Executive Board of Ghent University.

For existing ("legacy") applications and situations that are not consistent with this policy, due consideration must be given to the seriousness of the risks and actions necessary to reach conformity must be started within a reasonable period of time; i.e. no more than one year from the date of approval of this policy by the Executive Board.

Deviations from the policy in new applications or new projects must be reported to the information security counsellor. The latter will report on exceptions and deviations in the annual reports on information security.

8. Compliance

In the first instance, Ghent University counts on each end user's own sense of responsibility when complying with the current policy, in order to guarantee that personal data and confidential information are handled in a secure manner. Once end users have been adequately informed, if they then deviate from the policy or accompanying guidelines, and if this should lead to a security incident (e.g. a serious data leak), this can lead to formal (re)action if review of their conduct results in them being considered liable for sanctions.

If the end user is a student, formal measures may be taken in accordance with the disciplinary regulations.

If the end user is a contractual or statutory member of staff, he/she may be reprimanded in the context of a performance review. Formal (re)action is possible on the basis of disciplinary or employment law.

The end user's civil liability is subject to the relevant rules that apply in general. The general principle is embodied in Article 1382 of the Civil Code and reads: "*Every human act that leads to damage to another party must be compensated by the person who is responsible for the damage*."

Both contractual staff (under Article 18 of the Act of 3 July 1978 on employment contracts (WAO)) and statutory staff (under the Act of 10 February 2003 on the liability of, and for, people employed by public entities) are only liable for fraud or major negligence in the event of damage being incurred, and staff will only be liable for minor negligence if the damage occurs on a regular, rather than accidental, basis.

9. Support

The information security counsellor at Ghent University is the single point of contact for explaining the gist of this policy document, in case you have any questions or comments, in case problems have to be solved, and in case of any special situations within the framework of this policy document.

The information security counsellor may refer you for specialist advice.

10. Supervision

In accordance with privacy legislation the information security consultant at Ghent University is authorised to supervise the secure handling of personal data at Ghent University.

Accordingly, the information security consultant may organize random audits to check the secure handling of personal data processed at Ghent University.

11. Authorisation

This document has been submitted to the relevant management and advisory bodies of Ghent University:

A first draft with a number of discussion points was submitted to the ICT Committee, dated 27 February 2015.

Following further consultation and integration of suggestions and comments, the document was re-submitted to the ICT Committee on 26 June 2015. This was followed by a positive recommendation by the latter.

The Dutch language version of this document was approved by the Executive Board on 10 July 2015 and accepted by the negotiation committee for university staff (Dutch abbreviation: POC) on 30 September 2015.

12. References and sources (all in Dutch)

Privacy legislation can be consulted:

on the website of the Privacy Committee, under the heading "Legislation and Standards":
http://www.privacycommission.be/nl/wetgeving-en-normen

on the website of the Flemish Supervisory Commission, under the heading “Legislation”:
http://www.vlaamsetoezichtcommissie.be/wetgeving.php

This document refers in particular to:

The Act on the protection of privacy in relation to the processing of personal data (the Belgian Privacy Act) of 8 December 1992:
http://www.privacycommission.be/sites/privacycommission/files/documents/CONS_wet_privacy_08_12_1992.pdf

The Royal Decree implementing the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data dated 13 February 2001:
http://www.privacycommission.be/sites/privacycommission/files/documents/CONS_kb_uitvoering_privacywet_13_02_2001.pdf

Documents and forms on security:

Reference measures for the protection of all processing of personal data:
http://www.privacycommission.be/sites/privacycommission/files/documents/referentiemaatregelen_voor_de_beveiliging_van_elke_verwerking_van_persoonsgegevens_0.pdf

Declarations of conformity for the security of the information system (CBPL):
http://www.privacycommission.be/sites/privacycommission/files/documents/toelichting-conformiteitsverklaring-rr_0.pdf
http://www.privacycommission.be/sites/privacycommission/files/documents/toelichting-conformiteitsverklaring-fo.pdf
http://www.privacycommission.be/sites/privacycommission/files/documents/toelichting-conformiteitsverklaring-stat_0.pdf

Form for the “Assessment of the security of the information system for the protection of personal data” (VTC):
http://vtc.corve.be/docs/evaluatieformulier_beveiliging.doc

13. Addendum 1:

10 points for safely working with IT in practice

1. Use **a trustworthy device** (desktop, laptop, notebook, tablet, smartphone,…) **which is sufficiently secure**. This means:

    - The operating system and installed applications have the latest updates.
    - Applications that are not used are deleted.
    - Professional anti-malware (anti-virus, anti-spyware,…) with the latest updates is active (compulsory for desktop, laptop and notebook).
    - The anti-malware software occasionally performs a full scan besides the regular quick-scans or incremental scans.
    - Sign in to the device with a regular user account without extensive rights (so no administrator account). Sign in with your Ghent University account on any appliance configured by DICT.
    - To log on to Ghent University applications, always use your own Ghent University account, and enter these credentials only for known, reliable applications and authentication systems such as CAS and Athena.
    - Do not let others work on a personal device, except with clear agreements and using a different account (with limited privileges). If family members or third parties use the same device, this should be done using a separate account.

2. Within the buildings of Ghent University, you work on **a trusted network that is adequately protected**:

- either a fixed (wired) network connection (LAN) of UGentNet
- or a WiFi connection with EduRoam.

3. **Protect your Ghent University account** and the associated login data (username and password):

    - Use a strong password and change it at least once a year.
    - Keep your own password strictly confidential. It is forbidden to share your personal login with others, even to those you trust.
    - NEVER give the login data of your own account to others, not even close colleagues. Instead, make use of the proxy functionality of certain applications.
    - Never use the password of your Ghent University account for other services, not internally and certainly not externally.
    - Do not let anyone work with your personal account.
    - Remember to log out after you have used a public desktop.
    - Avoid the use of the “remember passwords” functionality of your web browser.
    - Lock or log out of your computer at work when you leave your desk for a while.
    - Never save your Ghent University password in readable form. Do not write your password anywhere and do not store it in a file. Never send your password by e-mail.

4. Be fully aware of **common risks and hazards**:

    - Do not open executable files that you do not trust completely. These may contain malware (virus, spyware, ransomware …).
    - Do not respond to suspicious invitations (so-called phishing) to disclose confidential data (e.g. login data).
    - Avoid questionable websites, which may infect your device with malware.
    - Set at least a security PIN on tablets and smartphones. That is a first measure to prevent worse if the device were to end up in the wrong hands.

5. **Use the central disk space/storage (personal disk space and shares) offered by DICT** instead of storing files locally on your own IT resources (hard disk of desktop or laptop, USB stick, external hard disk,…)

    - Avoid creating and working with local copies of data.
      Besides the problem of back-up and synchronization, there are serious security risks in terms of confidentiality involved (e.g. when you lose your device or when it is infected with malware). That risk might be mitigated by encrypting local data with cryptographic tools, but this can be rather complex and it gives a false sense of security if this is not carried out correctly.

    - The security of data on central infrastructure is guaranteed by the DICT specialists. They protect the central storage against unwanted access, the data is also protected against unwanted change or loss thanks to various back-up procedures.

    - **Please note:** the W:drive (www) for personal web space is accessible publicly & worldwide!

6. **Preferably work with the applications offered on Athena.UGent.be (Citrix technology)**

    - This ensures that you can use your central disk space effectively and productively.

    - Processing data on the central storage via applications offered on the Athena platform is a much safer alternative than editing your copies locally. The security of data and processing on the central infrastructure is guaranteed by the DICT specialists.

7. **Install as few additional applications as possible on your devices**, and certainly nothing that is downloaded from the internet without any security guarantees or sent via e-mail. This reduces the risk of infections with malware.

8. Do not use **external cloud services** to store personal data or confidential information unless you encrypt this data in a secure and reliable manner using cryptographic tools.

    Read the Terms of Use / Terms of Service and Privacy Policy, and consider the information security risks before you use external cloud services, including DropBox, iCloud, Google Drive, OneDrive (SkyDrive) for important, work-related information.

9. **You carry responsibility** for working with information in a secure manner. **Therefore, consider the information security risks** related to the material you work with, particularly if you work with personal data or confidential information.

   Even if you think you work in a sufficiently secure manner, for example on a laptop configured by DICT specialists, it is necessary to assess possible risks using common sense.

10. **Inform the DICT Helpdesk as soon as possible** if you suspect a **data leak,** as a result of which confidential information might have ended up in the wrong hands, or if you notice any other **information security incident**.

    Report any **stolen or lost IT equipment,** including smartphones and tablets, to the DICT Helpdesk (who may help you further). In such case we urge you to change your Ghent University password at the earliest opportunity.

14. Addendum 2:

10 points for safely managing servers and services at Ghent University

(for system administrators in faculties, departments and central administration)

1. **Hardware and operating system** of each server must be **effectively protected**:

    - The unit is in a **safe location**:
        - protected against unauthorized physical access;
        - protected against physical damage caused by heat, fire, water, dust, …
        - For that reason, the unit is accommodated or set up in a central data centre of Ghent University.

    - The operating system always has the latest updates.

    - Features of the operating system that are never used, are removed.

    - Unnecessary services are disabled.

    - Legacy operating systems that are no longer supported may no longer be used. To this end, a migration is to be provided to a system that offers sustainable security guarantees. If necessary, make an appointment with the DICT specialists for advice.

2. **Applications** on each server must be **effectively protected**.

    - All installed applications have the latest available updates.

    - For off-the-shelf applications and components (add-ons): regular (or automatic) checks must be carried out to see whether there are vulnerabilities known and described (e.g. via Common Vulnerabilities and Exposures (CVE)). Available updates and patches must be applied as soon as possible.

    - For custom developments (in-house or outsourced), check whether they are sufficiently protected against the vulnerabilities of the Open Web Application Security Project (OWASP) Top 10, for example SQL-Injection and Cross-Site Scripting.

    - Custom systems with personal data and confidential information must be subjected to an additional safety check before being produced (in consultation with the information security counsellor).

3. **Network access** to servers must be **effectively protected**:

    - The system is connected to UGentNet via a fixed (wired) network connection (LAN).

    - Restrict access to the device at network level:

        - Make the right choices when registering the device: intranet (server UGent) or internet (server Internet). Only select Server Internet if this is necessary for the intended services.
        - Only leave those network ports open that are required for the intended services.
        - Avoid the internet-wide opening of network protocols and network applications that enable your system to be managed remotely, such as SSH, RDP or web-related management tools. Only open them for specific subnets within UGentNet and for access via VPN.

    - Provide a sufficient level of intrusion detection and follow its results.

4. **Protect your accounts** and their associated login data (username and password) on all systems.

    - Protect, in particular, system administrator and root accounts. Always use strong passwords. Regularly choose a new password.

    - For Ghent University user accounts, only use the authentication mechanisms offered centrally by DICT: Central Authentication Service (CAS) or Active Directory authentication and OAuth for mobile applications.

    - It is prohibited to set up login forms yourself with which Ghent University account information is requested.

    - If a Web system for self-registration is provided (independent of CAS and AD), point out to the users that it is prohibited to register the same login data (username / e-mail address and password) as those of the Ghent University account. Do not allow anonymous self-registration.

    - Take the necessary precautions for the security of credentials, which should always be encrypted. Web authentication should always run via https (and with a correct server certificate).

5. The system administrator should be sufficiently **aware of common risks and hazards**.

    - Since servers are prime targets for hackers, configure sufficient logging and monitoring, and regularly check the logs and results of monitoring. Implement available security updates as soon as possible. Keep track of Common Vulnerabilities and Exposures for your systems.

    - When it is determined that a server has been hacked, it is often difficult to establish to what extent the system has been compromised and whether secondary Malware has been introduced (e.g. remote command and control software). That is why it is appropriate to run a clean install after an incident. Bear this in mind in advance.

6. Use the central infrastructure, platforms and applications offered by DICT.

- The basic security of the central infrastructure, platforms and applications offered by DICT is guaranteed by the DICT specialists.

- For existing and/or legacy systems that are not central, make an appointment with the DICT specialists to migrate them to the central infrastructure.

7. Follow recognized best practices for securing servers and services.

- Find the right balance between system hardening (against known and unknown threats) with different layers of protection ("defence in depth") and good maintainability.

- Consult security benchmarks and standard security configurations specifically for each operating system.

8. **Local system operators (within a department, faculty or within central administration) carry an important share of the responsibility** for the security of the systems under their management, including the security of the data processed through them.

   That is why local system operators must consider, and responsibly handle, the information security risks associated with the systems they manage, particularly if those contain personal data or confidential information.

9. **Together we are strong**:

    - At the beginning of each IT project, take the initiative to contact relevant stakeholders and also DICT in particular.

    - Maintain contact with, communicate with and consult, whenever necessary, fellow-system operators at Ghent University, the DICT specialists and the information security counsellor.

10. **Inform the DICT Helpdesk as soon as possible** if you suspect a server has been hacked, or if you notice any other **information security incident**.

    This is particularly important for critical systems, or systems through which personal data or confidential information could end up in the wrong hands.

15. Addendum 3: Working securely with personal data and confidential information in practice

Personal data and confidential information must be stored and processed in a way that guarantees the three key aspects of information security:

- Maintaining confidentiality, so that data leaks can be avoided and the information is not leaked to persons who do not have permission to consult the data;

- Guaranteeing integrity (accuracy and completeness) of the information;

- Ensuring availability, by actions such as taking appropriate storage measures (back-up), amongst other things.

It is proposed, therefore, to store such data within the central IT environment managed by DICT, where the necessary measures are implemented, in order to guarantee the above security setting.

The following brief guideline has been compiled in the context of applications for prior authorisation by the Privacy Commission for retrieving personal data from external sources, but is also more generally applicable. It indicates how the information flow and processing can be carried out in a secure manner, and how unwanted data replication can be prevented.

Transfer and storage of original source data from external databases

Source data from external databases containing personal data are transferred to a designated electronic storage within the central storage offered by DICT in a controlled and secure manner ("extra shared disk space = share" – see below).

Example: transfer via secure hard copy:
The data is transferred on to CD, DVD or USB stick as an encrypted file.
The password used is transmitted orally. After delivery of the medium, the protected files are transferred to the central storage within the Ghent University network.

The original medium with the source data is retained for a short period of time in a secure manner until such time as it is ascertained that the source data has been included in the back-up system (typically, this takes less than a day).

Thereafter, the information on the original medium can be deleted or destroyed. If the medium is a CD or DVD, DICT can help in its destruction using a CD-ROM shredder.

If there are good reasons for keeping the original information for longer, a suitable storage strategy is chosen, possibly in consultation with the information security counsellor.

Secure storage on central disk space offered by DICT

Besides the personal disk space offered in the central storage, Ghent University staff may apply for shared network disks ("shares"). This functionality is documented on the intranet web pages of the DICT helpdesk. See (among other)
https://helpdesk.UGent.be/netdisk/shares.php (in Dutch)
https://helpdesk.ugent.be/netdisk/en/shares.php (in English)

Both the personal disk space and the shares are on the central storage infrastructure provided by DICT. Any data stored on that infrastructure is secure and is automatically included in an effective and reliable back-up system.

A share is to be requested via a web form (”Aanvragen extra share”), upon which a coordinator and the other users of the share are assigned.

Access to the shared network disks is arranged on the basis of Ghent University accounts. When the share is created, the access rights are set automatically so that both the coordinator and all the other users of the share have full control over the share. This also means that they can change and restrict access rights, but only for the registered users of the share in question.

Users who are not listed in the application have no access.
If new users need to be added, or existing users need to be removed at a later date, the same procedure must be followed as that for a new application via the Web form.

It must be ensured that the confidential information of users who are removed from the list is permanently erased from IT resources (see below “Rules for the safe elimination of data”).

Example of use: storage of original source data (e.g. personal data obtained following prior authorization):

After a share is created, one of the registered users ensures that a separate folder is created to which the original source data can be transmitted. Once the source data has been transferred correctly, access to the folder with the source data can be restricted to read-only for all users.

Secure processing by means of applications offered via Athena

DICT offers software packages via the Athena platform (SPSS, SAS, R,…).
The Athena platform uses Citrix technology, a network technology whereby the applications are installed on central servers. To use the applications, the local device only needs a Citrix client program. When Citrix technology is used (in combination with central storage – either the personal disk space or shares), only screen images, mouse movements and keystrokes are sent securely across the network.

As a result, it is possible to work effectively and the level of security for processing personal data and confidential information is good. It is no longer necessary to take copies of the data and process it locally, with all the risks and disadvantages that this entails.

Secure disposal and/or destruction of data

When personal data or other confidential information are to be permanently removed, this is to be done in a way which means that it can no longer be retrieved with existing technology and with reasonable effort.

A specific guideline will be drawn up in due course for the secure and permanent removal of confidential data and the decommissioning of depreciated IT equipment, such as PCs, servers, datacentre equipment and smartphones.

It should be taken into account that data included in DICT's central back-up system is retained until it is eventually automatically deleted.