
SLU
SCIENCE AND EDUCATION FOR SUSTAINABLE LIFE

Challenges with attaining a satisfying level of electronic appraisal

SLU, LK/documentation, R.Arovelius, K.Pettersson
2019-07-01, Dundee

Outline

- Appraisal and appraisal rules at Swedish universities
- Classification schemes and validation of information
- GDPR and digital public records
- Appraisal of digital records and data
- Levels of destruction
- Possibilities for satisfying level of appraisal

The Swedish Legislation and Appraisal

The principle of public access

- Part of the Swedish Constitution.
- The Freedom of the Press Act (freedom of information)

sets out the principle of public access to official records for the general public and the mass media.

Freedom of information

- Possibility to scrutinize the activities of government on all levels – national, regional and local.
- Some records can be kept secret – e.g. if they involve matters of personal security, research co-operation or likewise.

The format of records does not matter.

Rules on Appraisal

- General rules and the regulations

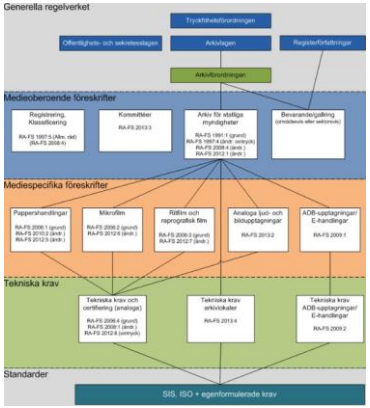
General

Media neutral

Media specific

Technical regulations

Standards



The Freedom of the Press Act

The Public Access & Secrecy Law

The Archival Law

The Archival Decree

The Register Legislation

The Regulations on Preservation and Appraisal

The main rule - preservation

- The main rule for management of public records is permanent preservation.
- No particular motives for appraisal within the Archival Law.
- Public records might be deleted if no longer needed for the administration, legal matters and research.

https://riksarkivet.se/vardera-och-gallra

https://se.dreamstime.com/illustration/lagbok.html

When possible to delete

- Deletion possible according to the particular legislation as a decree or law.
- The National Archives of Sweden is in charge of regulation on appraisal at governmental authorities.
- In some cases common national regulations are in force taking over all other rules.

Appraisal at the university

- Adaptation on the general rules from the National Archives.
- Application for specific rules on appraisal if no general rule possible to apply.

https://internt.slu.se/stod-service/admin-stod/juridik-dataskydd-och-informationshantering/dokument-och-arkiv/verksamhetsomraden-och-handlingstyper/

Appraisal adaptation

SLU KS 2013:1-1

- Process
- Type of record
- Time period
- Valid appraisal rule
- Date of deletion
- Person reposponsible

Process	Handlingstyp	Handlingarnas tidsomfång	Gallras enligt *	Gallrings-datum	Gallrat av

*Gallring får ske efter att följande beslut beaktats:

Riksarkivets beslut

1. RA-MS 2013:7 Riksarkivets föreskrifter om gallring hos Sveriges lantbruksuniversitet
2. RA-MS 2007:68 om upphävande av vissa myndighetsspecifika föreskrifter om gallring och överlämnande av handlingar m.m.
3. RA-MS 2005:31 om återlämnande av vissa ansökningshandlingar hos universitet och högskolor.
4. RA-FS 1991:6 (ändrad RA-FS 1997:6 och RA-FS 2012:2) Riksarkivets föreskrifter och allmänna råd om gallring av handlingar av tillfällig eller ringa betydelse (kräver tillämpningsbeslut se punkt 4 nedan).

SLUs tillämpningsbeslut:

1. Bevarande- och gallringsplan Dnr SLU ua 22-1373/07 (2007-07-23) för forskningsmaterial enligt RA-FS 1999:1 om gallring av handlingar i statliga myndigheters forskningsverksamhet.
2. Gallrings- och dokumenthanteringsplan för räkenskapsinformation enligt RA-FS 2015:2, SLU ID: SLU.ua.2016.2.1.2-2402
3. Gallrings- och dokumenthanteringsplan för studerandehandlingar Dnr SLU ua 22-2360/09 (2009-08-24) enligt RA-FS 2008:3 om gallring och återlämnande av handlingar vid universitet och högskolor.
4. Lokala gallringsbeslut gällande handlingar av tillfällig eller ringa betydelse för SLU och/eller beslut för universitetsadministrationen Dnr SLU ua 11.12-2640/01, 1999-03-09 och 2001-06-25 (enligt stöd av RA-FS 1991:6 och ändring 1997:6, 5§).

Scanning

- Change on media means deletion of records.
- Particular application for appraisal on scanned records.

https://riksarkivet.se/gallring-efter-skanning

GDPR and appraisal

- Appraisal on personal data according to the rules in the GDPR.
- Archival criteria for preservation overrule (revoke) reasons for appraisal according to the GDPR.

Levels of destruction

Distinctions according to Swedish lawyer Håkan Nordling (2015):

- Software
  - The information is flagged as deleted.
  - A pointer to the information is removed.
  - The information is over-written.
- Hardware
  - Degaussing of data carriers.
  - Physical destruction of data carriers.
- We will focus on software-based methods of destruction.

Information is flagged

- Examples
  - Moving a mail or a file to the trashcan.
- It is easy to recover the information with simple commands.
- Thus, records are still stored in the sense of Swedish law.
- Personal data are still processed in the sense of GDPR.

Pointer removal

- Pointers to the information are removed in a database.
  - Thus, the information *may* be overwritten with new information.
  - However, this is not automatically done, at least not immediately.
- Examples
  - The file system is a database with file metadata, e.g. pointers to disk areas where file contents are stored.
  - Remove a file in Explorer without moving it to the trashcan.
  - Run `rm [file]` in a Unix-like system (Linux/BSD/macOS).
  - Delete records in a database at a level above the file system (e.g. `DROP` in a SQL database).

Information recovery

- File systems with metadata journaling (NTFS/ext3/HFS).
- Grep device files in a Unix-like system, order to gain access to the disk at a level below the file system.
  - Example after ArchLinux Community (2018): `grep -a -C 200 -F 'sick leave' /dev/sda1`
- Potential records (e.g. lists generated from a database) in the sense of Swedish law cannot be recovered “in a routine way”?

SLU

Overwriting

- File or disk contents is overwritten with e.g. zeros or random bits.
- Example
  - `dd` and `shred` in Unix-like systems.
- It is sometimes claimed that multiple passes are needed for optimal security. However, this is doubtful (Gutmann 1996).

Limits of overwriting I

- Abstractions between file system and hardware (cf. Fischer and Schönberger (2017)) may lead to new data not being written in-place.
  - File systems with cache, “copy on write”, RAID, compression, and so on.
  - Logical volume management below the file system (using the techniques mentioned above).
  - Networking and virtual systems (with servers/host systems using the techniques mentioned above).
  - Similar techiques implemented in hardware: hardware RAID, SSD (more on that below).

Limits of overwriting II

- This might lead to overwriting not being more effective than pointer removal when it comes to preventing information recovery.
- Overwriting disks may be more secure than overwriting ordinary files, e.g.: `dd if=/dev/zero of=/dev/da0 bs=4194304 seek=1024 count=399559` (recently used for the unauthorized wiping of a commercial email service (VFEmail 2019)).
  - But a disk may contain information with varying rules of appraisal.
  - Bad sectors are missed.

Limits of overwriting III

- SSD drives abstract away from the addressing in software (e.g. for “wear levelling”, in order to prevent areas of the disk from being worn out prematurely).
  - Thus, overwriting the disk with system commands like `dd` may not be effective.
  - However, special equipment, for direct access is needed in order to recover information. In such cases, records may not be stored in the sense of Swedish law.
  - In order to prevent such recovery, the drive’s internal routines for “Secure Erase” have to be called (e.g. with `hdparm`).
  - However, these routines are not standardized and may not be as secure as the name suggests (Wei et al. 2011)?

What is to be done?

- Risk appraisal is neceesary (e.g. for processing personal data).
- Be cautious with cloud services.
- Be cautious with SSD drives?
- Use hardware-based methods of destruction to a greater extent?
- Encrypt sensitive data (destroying decryption keys is easier than destorying whole records)?

References I

ArchLinux Community. 2018. “File Recovery.” 2018. https://wiki.archlinux.org/index.php?title=File_recovery&oldid=528916.

Fischer, Werner, and Georg Schönberger. 2017. “Linux Storage Stack Diagram.” 2017. https://www.thomas-krenn.com/en/wiki/Linux_Storage_Stack_Diagram.

Gutmann, Peter. 1996. “Secure Deletion of Data from Magnetic and Solid-State Memory.” In *Proceedings of the 6th Conference on Usenix Security Symposium, Focusing on Applications of Cryptography - Volume 6*. SSYM’96. Berkeley, CA, USA: USENIX Association. https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

References II

Nordling, Håkan. 2015. “Schrödingers Handlingar : När är En Elektronisk Handling Gallrad?” Stockholms universitet; Juridiska institutionen. http://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Asu%3Adiva-121372.

VFEmail. 2019. “VFEmail on Twitter.” February 11, 2019. https://twitter.com/VFEmail/status/1095021927972909056.

References III

Wei, Michael, Laura M. Grupp, Frederick E. Spada, and Steven Swanson. 2011. “Reliably Erasing Data from Flash-Based Solid State Drives.” In *Proceedings of the 9th Usenix Conference on File and Storage Technologies*. FAST’11. Berkeley, CA, USA: USENIX Association. http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf.