

Joint filing principles at ST

Contents

Purpose.....	2
Why ECDM?	2
When should you use WorkZone?.....	2
What is a case?	2
When do you need to create a case?	3
How to define a case (single-case principle).....	3
Naming cases	3
Case number (reference number)	3
Protection of cases (insight)	3
Parties.....	3
Documents	4
Classification of documents.....	4
Obligation to record	4
Regarding emails	4
Deleting documents filed.....	4
Non-digital documents	4
Overall framework.....	5
More information	5

Purpose

The following describes the general principles for why and when you as an employee should work in AU's electronic case and document management (ECDM) system, WorkZone. This is a brief description of the background and requirements for data protection as well as filing and documentation obligations.

Why ECDM?

As a public authority, AU has to document the organisation's activities and existence in an approved ECDM system (electronic case and document management system). AU uses WorkZone, which can also be used as an ECDM system.

You can use a system other than WorkZone, provided you are working in an approved filing system for which you have entered into a submission agreement with the Danish State Archives. Note that folders in Outlook, private drives, shared drives, One Drive, USB sticks etc. are *not* approved specialist systems. Case-relevant emails and documents from these drives should therefore be filed in WorkZone.

When should you use WorkZone?

All employees are subject to a filing obligation, and as an employee, you should therefore file all documents, letters, incoming and outgoing emails, memos, meeting minutes, telephone notes etc. relating to AU's internal activities as well as external collaborations.

If you are in doubt as to whether what you are working on should be filed in WorkZone, ask yourself the questions below. If you can answer 'yes' to any one of them, you should file information and documents for the assignment in a case in WorkZone.

Are you working on an assignment in which:

- you collect general, sensitive or confidential personal data about a person, e.g. CPR number, name, address, occupation or illness?
- complaints or requests for right of access to documents may subsequently arise?
- you or others will later have to make decisions or rulings? For example, this may be in relation to recruitment of employees, rejection/authorisation for credit transfer, applications for funding or to plan research projects, approval of a rule/strategy/policy, determination of a work process or planning a call for tenders, or establishment of internal rules and procedures.
- you collect/record case-relevant knowledge that you or your colleagues may need to perform the task or to perform similar tasks in the future?
- you prepare an agenda/minutes, for example, for an internal department or management meeting?
- you are working with (draft) external agreements of any kind, negotiations, contracts, or similar?

What is a case?

A case is like a physical folder in which you have all the documents, emails, memos, data on parties etc. you collect and note to perform a task/project.

When do you need to create a case?

You should create a case when you start on a task/project. When you receive a document/write a memo based on a telephone call, or start collecting knowledge/describing the current status for a presentation, you should set up a case and save your documents, memos etc. on the case.

When you create a case, you should add various data to the case, based on the topic covered by the case, e.g. reference number, title, responsible unit and case officer.

How to define a case (single-case principle)

Filing at AU is according to the single-case principle. In other words, the individual case only contains the documents, data on parties, notes etc. relating to one specific task. For instance, you must always set up complaints cases and cases concerning access to documents as independent cases.

Once the individual assignment has been processed, you should conclude the case.

The single-case principle ensures that no information is stored in cases for which the information is not relevant. It also ensures clarity as to which acts and parties have led to which decisions. The principle also helps to ensure that we do not retain ordinary, sensitive or confidential personal data for longer than we are authorised.

Naming cases

The name of a case should be brief and descriptive, based on the topic of the case. This makes it easier for yourself and others to search for the case later.

AU has specific rules for naming cases in several fields.

Case number (reference number)

When you create a case, the case must have a reference number based on the AU file chart (journalplan). The file chart is divided into main groups, followed by topic groups and finally case groups.

The file chart is embedded in WorkZone, so when you create a case, you just have to select the case group you are about to work on, and WorkZone will automatically create a case number.

Protection of cases (insight)

In order to secure possibilities for cooperation and knowledge sharing across AU, the topic cases in WorkZone are generally open to all employees.

Of course, cases involving sensitive or confidential personal data are not open. Student and staff cases are therefore automatically created with restricted access.

Note that it is only permitted to access cases that are relevant in a work-related context. As the system is logged, you should therefore be able to justify the relevance of the case in relation to your tasks. If you read cases without justification that are not relevant to your work, this will be considered as a breach of your responsibilities and may result in disciplinary action.

Parties

Parties in a case may be persons, companies, organisations, etc. These can be set up in WorkZone as contacts, and when they are linked to a case, they are called parties.

Important: As a public institution, we must be able to respond appropriately if someone asks the university about what information we have on them. We can only answer such questions if the person is linked to all relevant cases as a party.

Documents

All documents (emails, Excel, Word or PowerPoint files) that are relevant to case processing should be stored in WorkZone. The same applies to pictures, drawings, sound files etc.

Classification of documents

AU has made a security decision to classify all the data we process at AU. This also applies to the documents we file in WorkZone.

Data is classified as public data, internal data, sensitive data or confidential data, respectively. Classification of data is a key aspect of data security. If we do not classify our data and treat data in relation to its respective classifications, we risk compromising personal data or having to withdraw patent applications.

Read more about classification of data on the AU website:

<https://medarbejdere.au.dk/en/informationsecurity/classification-of-data/>

Obligation to record

As an AU employee, you have an obligation to record. The obligation to record helps to ensure that later it is possible to clarify what happened in a case (documentation), and check effectively whether, as an authority, AU has acted correctly (control).

This means that when you receive information (orally or in any other way) about the actual basis of a case or external expert assessments of significance to determination of the case, you must write a memo and file it on the case in WorkZone. The obligation to record also applies in relation to significant steps in case processing.

Regarding emails

Emails are also counted as documents, so if you send or receive emails that are relevant to your assignment/project, they should also be saved in WorkZone.

AU has made a security decision that staff at AU may not store sensitive and confidential personal data in Outlook for a longer period of time than is relevant for the relevant case, **and for a maximum of 30 days**.

The Ombudsman also stipulates that emails should generally be filed as quickly as possible and by no later than seven business days after receipt/dispatch. This means that you should keep an ongoing record of your inbox and file emails when you send them. If you have a long email correspondence on the same topic with the same recipient, you need only file the last mail received/sent.

Nat-Tech also recommends that everyone remembers that external parties should be able to read our emails, and that private messages should be sent so that they are not linked to cases in WorkZone.

Deleting documents filed

You can delete drafts, but you cannot delete documents filed in WorkZone. If a document has been filed on an incorrect case, you should move it to the right case.

If you have filed a document by mistake, contact [your](#) superuser.

Non-digital documents

If a case involves very large physical documents that cannot be scanned, e.g. maps, note in the relevant case where the physical document is available.

Overall framework

- Filing Instructions Aarhus University 2016-2021
- AU rules for filing at departments and department-like centres (2015)
- EU General Data Protection Regulation
- Danish Data Protection Act
- Danish Access to Public Administration Files Act
- Danish Public Administration Act
- Danish Archives Act

More information

Link to Nat-Tech's Click Guides:

<https://medarbejdere.au.dk/en/administration/hr/hr-systemer/esdh/vejledninger/joint-filing-principles-at-nat-and-tech/nat-and-tech-guidelines-and-descriptions/>

Link to HR IT's guidelines and descriptions of filing practice at departments and in connection with projects (in Danish only):

<https://medarbejdere.au.dk/administration/hr/hr-systemer/esdh/vejledninger/>

Link to AU's staff pages on data security: <https://medarbejdere.au.dk/en/informationsecurity/>