The Danish Data Protection Agency’s 12 minimum requirements for personnel administration.

1. Describe how you protect personal data in personnel administration and how you have implemented in practice item 2-12.
   Stated in “Confidentiality instructions for HR staff” and “Confidentiality instructions for secretarial staff with HR administrative tasks” and “Information security policy and rules”.

2. Access to data must be limited to persons who have a legitimate need to access the data.
   Document concerning “Assessment of HR copy recipients” has been drawn up.

3. Staff who handle personal data must receive instruction and training in what they may do with the data and how they should protect the data.
   Stated in “Confidentiality instructions for HR staff” and “Confidentiality instructions for secretarial staff with HR administrative tasks” and “Information security policy and rules”.

4. Personal data on paper, for example, in files and ring binders, must be kept in locked storage when not in use.
   Stated in “Confidentiality instructions for HR staff” and “Confidentiality instructions for secretarial staff with HR administrative tasks”.

5. Passwords must be employed to access PCs and other electronic devices containing personal data.
   To be secured by AU IT and stated in “Information security policy and rules” item 4.4.

6. All failed attempts to access IT systems containing sensitive personal data must be registered.
   To be secured by AU IT and HR IT.
7. If personal data is stored on a USB key, the data must be protected, for example, with a password and encryption.
   Stated in “Information security policy and rules” item 5.2.

8. PCs connected to the internet must have updated firewall protection and antivirus software installed.
   To be secured by AU IT. Stated in “Information security policy and rules” item 5.7.

9. If website forms are used in which sensitive personal data and civil registration numbers can be entered and submitted, encryption must be employed.
   To be secured by the system administrator: AU IT or HR IT.

10. If sensitive personal data and civil registration numbers are sent by email over the internet, the Danish Data Protection Agency recommends using encryption.
    See “Confidentiality instructions for HR staff” and “Information security policy and rules”. Guidelines will be drawn up by AU IT.
    AU HR uses e-Boks where possible. Emails will be sent to the secure mailboxes provided.

11. During repair and servicing of data equipment as well as disposal of data media containing personal data, necessary measures must be taken to ensure the data is not disclosed to unauthorised parties.
    See “Information security policy and rules” item 4.4.

12. When using external data processors to process data, Section 42 of the Danish Act on Processing of Personal Data (Persondataloven) regarding written data processing agreements etc., must be complied with.
    To be secured by the system administrator.