BUS Framework Agreement Appendix

Organisational requirements and principles on data protection

A) Organisational requirements

The applicable legal data protection regulations for the protection of personal rights and the technical data protection requirements for the protection of data, hardware and software from destruction, loss and misuse shall be identified and implemented by the contractor. Data protection measures including technical and organisational measures shall be continuously documented (privacy policy, IT security concept).

Organisational responsibilities

- Transparent data processing must be ensured (e.g. privacy policy on the website)
- Permanent staff are bound to maintaining data confidentiality (data secrecy)
- Data protection training must be provided to staff
- The rights of data subjects (including providing information, correcting and erasing records, dealing with data breaches) must be ensured

B) Principles on data protection

The contractor shall observe the following principles when processing personal data:

1. **Lawfulness, proportionality, fairness, transparency**;
2. **Purpose limitation:** personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. **Data minimisation:** personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; personal data must be anonymised or pseudonymised, as far as this is possible according to the intended use and does not require disproportionate effort in relation to the desired level of protection;
4. **Accuracy:** personal data must be accurate and, where necessary, kept updated. Every reasonable step must be taken to ensure that personal data that are inaccurate, with regard to the purposes for which they are processed, are erased or corrected without delay;
5. **Storage limitation:** personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
6. **Integrity and confidentiality:** personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful destruction or accidental damage.