USX Cyber Data Protection Policy

Many data protection policies are unhelpfully long and simply reiterate large portions of legislation. USX Cyber Data Protection Policy is different: it aims to provide a concise and practical description of our data protection protocols.

USX Cyber data protection protocols aim to fully comply with both evolving industry best practices as well as Prevailing Law (defined below). USX Cyber reserves the right to update our data protection protocols through posting the latest version of the USX Cyber Data Protection Policy to our website.

This USX Cyber Data Protection Policy was last updated October 1, 2022.

Definitions

USX Cyber means USX Cyber, LLC a company organized under the laws of the Commonwealth of Virginia.

Prevailing Law means transnational, national, and local laws including, without limitation, the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, the UK Data Protection Act and Adequacy Regulations, the California Consumer Privacy Act, and the Virginia Consumer Data Protection Act.

Responsible Person means Frank Hughes, USX Cyber Chief Information Security Officer, who is responsible for data protection within USX Cyber.

Register of Systems means an index of all systems or contexts in which personal data is processed by USX Cyber.

1. Data protection principles

USX Cyber is committed that personal data shall be:

a. processed lawfully, fairly, and in a transparent manner in relation to individuals;
b. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes);

c. adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date (every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay);
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes subject to implementation of the appropriate technical and USX Cyber measures required by Prevailing Law in order to safeguard the rights and freedoms of individuals); and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

2. General provisions

a. This policy applies to all personal data processed by USX Cyber.
b. The Responsible Person shall take responsibility for USX Cyber's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.

3. Lawful, fair, and transparent processing

a. To ensure its processing of data is lawful, fair, and transparent, USX Cyber shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals who have the right to access their personal data under Prevailing Law may do so and any such requests made to USX Cyber shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by USX Cyber must be done on one of the following bases under Prevailing Law: consent, contract, legal obligation, vital interests, public task, or legitimate interests.
b. USX Cyber shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in USX Cyber's systems.

5. Data minimization

a. USX Cyber shall ensure that personal data are adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
b. USX Cyber shall develop criteria to help reduce personal data and review these criteria at least annually.

6. Accuracy

a. USX Cyber shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, USX Cyber shall put in place an archiving policy for each area in which personal data is processed and review this process at least annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. USX Cyber shall ensure that personal data is stored securely using modern software that is kept-up to date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, USX Cyber shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to designated government authorities.

END OF POLICY