Jurisdiction	*Uzbekistan*
Date	*26 July 2022*
Law Firm	*Dentons Tashkent*
Name and Position of the person in charge	*Ulugbek Abdullaev* *Counsel*
Contact Information	*ulugbek.abdullaev@dentons.com, tashkent@dentons.com*

* We are planning to put the information on our website so that the viewers can reach out to you, directly, and if you don't mind, we will include the above contact information in the report. You may have more than one contact person.

Questionnaire

I. Law concerning protection of personal information

i. Does your country have a general law concerning the protection of personal information in the **private sector** at the present or in the near future?

*Yes, the comprehensive data protection law for both private and public sectors in Uzbekistan is the Law on Personal Data No. 547 dated 2 July 2019 (the "**Law**").*

ii. Does your country have a general law concerning protection of personal information in the **public sector** at the present or in the near future?

Yes, please see the answer to question i above.

iii. Does your country have laws concerning protection of personal information **which apply in individual (specific) sectors** at the present or in the near future? (If yes, please describe outline.)

No, there is not.

Where all of the answers to the question of I.(i), (ii) and (iii) is "no", please skip to IV.

II. The basic information of the regulation concerning protection of personal information.

i. Please fill in the blanks below about all the law concerning personal information mentioned at I..(please add a reply column as necessary,)

The title of the law ： *Law on Personal Data No. 547 dated 2 July 2019*

① The definition of "Personal Information"	*"information recorded on electronic, paper and (or) other tangible media relating to an identified or an identifiable individual"*
② The scope in which the	*It applies to relations arising from the processing and protection of personal data, regardless of the means of*

law applies	*processing, including information technology.*
③ The territorial scope	*Not defined.* *In general, the laws of Uzbekistan apply to nationals (citizens and legal entities) of the Republic of Uzbekistan, as well as to foreign legal entities that carry out activities on the territory of the Republic of Uzbekistan, foreign citizens and stateless persons situated on the territory of the Republic of Uzbekistan, unless otherwise provided by an international treaty of the Republic of Uzbekistan (article 44, the Law on Normative Legal Acts). Hence, depending on the exact circumstance, the national data protection law may also apply to organizations located overseas which process personal data of data subjects in Uzbekistan if they are found to be "carrying out activities on the territory of Uzbekistan" (for example, over the Internet) and the organization in Uzbekistan may need to comply with the law when it processes personal data of data subjects overseas.*
④ URL (please provide the URL officially posted by the government, English page is preferred, if available)	*https://lex.uz/docs/4396419 - in Uzbek language* *https://lex.uz/docs/4831939 - in English (unofficial and may not reflect the latest amendments)*
⑤ The **effective** date *	*2 July 2019 and amended as of 16 April 2021*

* If the law has been amended, please fill in the effective date of the amended law.

ii. If there are any special instructions about the laws, please describe them.

III. OECD Privacy Principles

i. If there are any provision of law which embody each OECD Privacy Principle in your country, please describe the outlines.
https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(a) Collection Limitation Principle

This principle means that there should be limits on the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Yes, the Law on Personal Data No. 547 reflects this principle: articles 5, 10, 12 and 31.

Article 5 states that the legality of the purposes and methods of personal data

processing is one of the main principles of the Law.
Article 10: The database of personal data is formed by collecting personal data necessary and sufficient to complete the tasks carried out by the owner and (or) operator, as well as by a third party.
Article 31: the owner and (or) operator must approve the composition of personal data necessary and sufficient for the performance of their purpose.

(b) Data Quality Principle

This principle means that personal data should be relevant to the purposes for which they are to be used, and, to the minimum extent necessary for such purposes, should be accurate, complete and kept up-to-date.

Yes, the Law on Personal Data No. 547 reflects this principle: articles 5, 11, 19 and 31.
Article 5 states that the accuracy and reliability of personal data is one of the main principles of the Law.
Article 11: personal data must be amended within 3 days from the date of subject's request and any incorrect personal data must be amended (corrected/deleted) instantly.
Article 19: Personal data must be accurate and reliable, and, if necessary, change and supplement.

(c) Purpose Specification Principle

This principle means that the purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Yes, the Law on Personal Data No. 547 reflects this principle: articles 5, 10, 19 and 30.
Article 5 states that the legality of the purposes and methods of personal data processing is one of the main principles of the Law.
Article 12 states that the use of personal data is carried out only for the previously stated purposes of their collection.
Article 19: The purposes of processing of personal data should correspond to the purposes previously stated during their collection, as well as the rights and obligations of the owner and (or) operator. The volume and nature of the

processed personal data should correspond to the purposes and methods of their processing. In the event of a change in the purpose of processing of personal data, the owner and (or) operator must obtain the consent of the subject to the processing of his data in accordance with the changed purpose. Article 30 states that the subject of personal data has the right to require the owner and (or) operator to temporarily suspend the processing of their personal data, in case the personal data is not necessary for the purpose of processing.

(d) Use Limitation Principle

This principle means that personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with (c) Purpose Specification Principle, except:

i) with the consent of the data subject; or

ii) authorized by law.

Yes, the Law on Personal Data No. 547 reflects this principle: article 5, 14, 18 and 31.

Article 5 states that the legality of the purposes and methods of personal data processing is one of the main principles of the Law.

Article 14 states that any disclose of personal data must be with the data subject's consent and defines that scope of disclosure (to an indefinite range of persons, including publication of in the media, posting on the Internet or providing access to personal data in any other way)

Article 18 states the grounds for processing the personal data, including the consent of the data subject and the other exhaustive list of cases authorized by the law.

Article 31: the owner and (or) operator must provide evidence of the consent of the subject to the processing their personal data.

(e) Security Safeguards Principle

This principle means that personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Yes, the Law on Personal Data No. 547 reflects this principle: articles 5, 12, 28 and 31.

Article 5 states that the confidentiality and security of personal data is one of

the main principles of the Law.

Article 12: The use of personal data by the owner, operator and third party is carried out only for the previously stated purposes of their collection, provided that the necessary level of protection of personal data is ensured.

Article 28 obliges the owner/operator not to disclose and share the personal data without the subject's consent and keep them on confidential basis.

Article 31: The owner and (or) operator must take the necessary legal, organizational and technical measures to protect personal data. The obligations of the owner and (or) operator, as well as a third party to protect personal data, arise from the moment of collection of personal data and are valid until their destruction or anonymization.

(f) Openness Principle

This principle means that there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and address of the data controller.

Yes, the Law on Personal Data No. 547 reflects this principle: articles 30 and 31.

Article 31: the owner and (or) operator must provide, upon request of the subject, information regarding the processing of his personal data and the opportunity for the subject to submit documents in electronic form to temporarily suspend the processing and (or) destruction of his personal data.

(g) Individual Participation Principle

This principle means that an individual should have the right:

i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller holds data relating to him;

ii) to have communicated to him, data relating to him within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

iii) to be given reasons if a request made under subparagraphs (i) and (ii) is denied, and to be able to challenge such denial; and

iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Yes, the Law on Personal Data No. 547 reflects this principle: articles 22, 23 and 30.

Article 22 lists the scope of information which the data subject may require from owner/operator to provide (purpose, method of processing, content, procedure, etc.) and cases when owner/operator may reject to provide such information (the data obtained publicly, the subject was previously informed, etc.)

Article 23 states when owner/operator must and is not required to notify the data subject on the purpose, methods, use of personal data.

Article 30: The subject of personal data has the right to:

- *know that the owner and (or) operator, as well as a third party, have their personal data and their composition;*
- *receive, upon request, information on the processing of personal data from the owner and (or) operator;*
- *receive information on the conditions for providing access to their personal data from the owner and (or) operator;*
- *apply for protection of rights and legitimate interests in relation to personal data to the authorized state body or court;*
- *give consent to the processing of their personal data and withdraw such consent, except as otherwise provided by this Law;*
- *give consent to the owner and (or) operator, as well as to a third party, to distribute their personal data in public sources of personal data;*
- *require the owner and (or) operator to temporarily suspend the processing of his personal data, in case the personal data is incomplete, outdated, inaccurate, illegally obtained or is not necessary for the purpose of processing.*

(h) Accountability Principle

This principle means that a data controller should be accountable for complying with measures which give effect to the principles stated above.

Yes, the Law on Personal Data No. 547 reflects this principle: articles 27, 27(1), 28 and 30.

Article 27 state that government ensure the protection of personal data and obliges owner/operator processing personal data to take necessary measures

for such purpose (not to disclose, prevent illegal processing, keep the personal data up-to-date etc.)
Article 27(1) states that the owner and (or) the operator when processing personal data of citizens of the Republic of Uzbekistan with the use of information technologies, including the Internet, must ensure their collection, systematization and storage in databases (technical devices) physically located in the Republic of Uzbekistan and registered with the national data protection authority of Uzbekistan in the prescribed manner.
Please see above for the summary of articles 28 and 30.

ii. If there are any sectors in which any laws exclude the application of each OECD Privacy Principle, please describe the outline.
No, there are no such laws. However, in general the Yes, the Law on Personal Data No. 547 (including the OECD Privacy Principles reflected in the law) does not apply to processing of personal data obtained in the course of investigatory, intelligence and counter-intelligence activities, combating crime, law enforcement, as well as combating money laundering.

(a) Collection Limitation Principle
—

(b) Data Quality Principle
—

(c) Purpose Specification Principle
—

(d) Use Limitation Principle
—

(e) Security Safeguards Principle
—

(f) Openness Principle
—

(g) Individual Participation Principle
—

(h) Accountability Principle
—

IV. Data Localization and Government Access

In your country, are there any systems having an impact on the rights of data subjects such as **comprehensive government access (e.g., limitation on the authorities' access to personal data for investigation purposes, and the safeguard is the attorney-client privilege)** to personal data or **Data Localization (e.g., rules requiring domestic installation and storage of servers and data)**? If yes, please describe them.

Government access *to privately held personal data is possible based on:*

a) *A court-issued warrant*
b) *a prosecutor-issued warrant;*
c) *other law-enforcement-agency - issued warrants in the pre-defined cases.*

Only locally licensed lawyers (i.e. "advocates") are privileged not to disclose any information, including the personal data to anyone under attorney-client privilege (art. 9 of the Law on Advocacy https://lex.uz/docs/58372#1427847)

Yes, Uzbekistan has data localization requirements mandating that the collection, systematization and storage of personal data of Uzbekistan citizens must be done on technical means physically located on the territory of the Republic of Uzbekistan and the database holding such qualifying data must be duly registered with the national data protection authority of Uzbekistan. Failure to comply with the data localization requirement may lead to restriction of online access to the web-site on the territory of Uzbekistan.

V. The Data Protection Authority

If there is the data protection authority, please write down the name and address of the authority

Name: *The State Center for Personalization under the Cabinet of Ministers of Uzbekistan*
Address: *160A Bogishamol str., Yunusabad district, Tashkent, 100053, Uzbekistan.*
Telephone: *not available*
Website: *pd.gov.uz*
Other information if any: