

# ClientAlert

## Corporate Law

January 2014

### New Personal Data Protection Law

On 21 May 2013, the Parliament of the Republic of Kazakhstan adopted the Law "On Personal Data" (the "**Personal Data Law**"), which entered into force on 25 November 2013.

The Personal Data Law affects all commercial and non-commercial legal entities in Kazakhstan, including governmental agencies, which collect, store and use personal information in relation to the individuals in their operations.

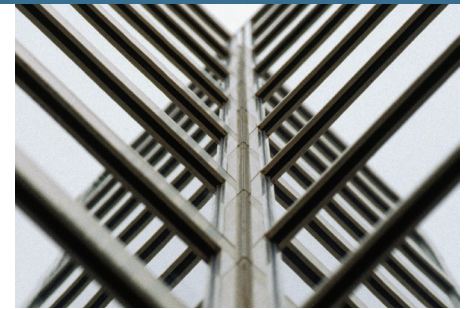
The Personal Data Law might be of the particular interest to Kazakhstan banks which transfer personal data collected from their customers who are private individuals to locations outside of Kazakhstan and process such information by using processing centers in foreign countries.

All entities affected by the Personal Data Law must bring their internal regulations into compliance with the requirements of the Personal Data Law within 3 months from the date it entered into force, i.e., by 25 February 2014.

#### Overview of key provisions

The key provisions of the Personal Data Law include:

- **Definition of Personal Data.** "Personal data" is defined as "data related to a specific individual or an individual who may be identified on the basis thereof and which are fixed on electronic, paper and/or other material objects." In other words, such information includes a person's surname, given name, father's name, ethnic group or nationality, gender, date and place of birth, individual identification number, legal address, residence address, contact data, identification document number, marital and family status, confirmation of the ownership of property, education, profession and biometrical data reduced to tangible form.
- **Collection and Processing of Personal Data.** Collection and processing include any actions to obtain, accumulate, store, amend, supplement, distribute, depersonalize, destroy or block (i.e., temporary suspension of the aforesaid actions) personal data.
- **Individuals' Consent.** Legal entities (the "**Authorized Users**") are permitted to collect and process personal data based on the consent of the individuals the data concern; however, the concerned individuals can revoke their consent at any time. The consent must be in written form or in the form of an electronic document or be granted otherwise by using protective means. Authorized Users must ensure that they take all measures which are usually used in their respective industries to protect communications with private individuals.



If you have questions or comments regarding this Alert, please contact one of the lawyers listed below:

Maxim Telemtayev  
Partner, Astana  
+ 7 717 258 26 50  
mtelemtayev@whitecase.com

Vilen Adjivefayev  
Local Partner, Almaty  
+ 7 727 258 26 50  
vadjivefayev@whitecase.com

White & Case Kazakhstan LLP  
Park View Office Tower  
77 Kunaeva Street  
Almaty 050000, Kazakhstan  
+ 7 727 258 26 50  
+ 7 727 258 26 51

White & Case Kazakhstan LLP  
3rd Floor Block A Business Center Q  
Kabanbai Batyr Street, 15a  
Astana 010000, Kazakhstan  
+ 7 717 255 28 68  
+ 7 717 258 26 50

## New Personal Data Protection Law

---

- **Specific Obligations.** Authorized Users must:
  - a) collect and process the personal data strictly for purposes which are necessary for their operations;
  - b) approve a list of the necessary personal data;
  - c) process the personal data only for the purposes for which it was collected;
  - d) delete the personal data after the reason for its collection is no longer relevant, for example, if an employment or client relationship is terminated. In such cases, the personal data should be deleted except to the extent otherwise required by law. For example, Kazakhstan banks are required to store certain data pursuant to the Resolution of the Agency for Control and Supervision of Financial Markets and Financial Organisations of the Republic of Kazakhstan dated 27 August 2005 No. 320;
  - e) undertake protective measures which (a) prevent unauthorized access to the personal data; (b) if unauthorized access cannot be prevented, detect such access in a timely manner; and (c) minimize any adverse consequences of such access;
  - f) within three (3) business days of an individual's request, provide a description of his/her personal data stored by the Authorized User or amend such data based on supporting documents provided by the individual; and
  - g) within one (1) business day from the receipt of evidence that the personal data was collected or processed illegally, block or delete such personal data.

### Cross-Border Transfers of Personal Data

Starting from 25 November 2013, personal data may only be transferred from Kazakhstan to a foreign country (including for purposes of processing) if such country protects personal data at either the national level (by adopting national laws and regulations) or the international level (through international treaties, for example, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981).

If no such protection is available, any cross-border transfer of the personal data will require the individual's specific consent.

The Personal Data Law does not specify the level of national protection which would be acceptable for the purposes of cross-border transfer and does not clarify whether the national protection needs to be provided through specific or general regulations. Therefore, a case-by-case analysis of national law is required for each country to which the personal data is to be transferred.

The Personal Data Law states that the cross-border transfer of personal data may be restricted or prohibited by the statutory laws of Kazakhstan.

### No Retroactive Effect

The Personal Data Law does not have retroactive effect, but it does state that any personal information collected and processed (including outside of Kazakhstan) prior to 25 November 2013 will be recognized as collected and processed in compliance with the Personal Data Law only if further collection and protection of such personal data complies with the requirements of the Personal Data Law.

### Liability for Breaches of the Personal Data Law

Following the adoption of the Personal Data Law, the Code on Administrative Violations introduced financial penalties for not complying with the new regulations. The penalties range from US\$600 to US\$3,600. Material breaches may also be subject to criminal liability. However, the liability has not yet been tested and there is no existing practice on how such liability would be enforced.

This Client Alert is provided for your convenience and does not constitute legal advice. It is prepared for the general information of our clients and other interested persons. This Client Alert should not be acted upon in any specific situation without appropriate legal advice and it may include links to websites other than the White & Case website.

White & Case has no responsibility for any websites other than its own and does not endorse the information, content, presentation or accuracy, or make any warranty, express or implied, regarding any other website.

This Client Alert is protected by copyright. Material appearing herein may be reproduced or translated with appropriate credit.