



New Data Protection Law Tightens Internal Compliance Investigations

Compliance with data protection regulations always requires a balance between freedom of information and privacy protection, both of which are guaranteed by the Constitution of Ukraine. In particular, Ukrainian laws provide that all individuals and companies are free to obtain, use, store and disseminate information to the extent that this does not violate rights and lawful interests of other individuals and companies.

Maintaining such balance could become a challenge for companies operating in Ukraine, especially when it comes to an internal review process, compliance investigation or the like. Accessing the personal data of employees without due process may be considered a violation of their privacy, which would result in several negative consequences for the company, namely impossibility to prove non-compliance or fraud, claims from employees, etc.

Thus, when it comes to an internal investigation or review, a company should invoke satisfactory safeguards ensuring observation of applicable data protection laws to protect the company from related risks.

Legal Regulation of Data Protection

The basic acts in the area of personal data protection are the *On Information Act of Ukraine of 2 October 1992* (the *Information Act*), and recently adopted *On Protection of Personal Data Act of Ukraine of 1 June 2010* (the *Data Protection Act*).

Under the general rule set out in the *Information Act*, the information is deemed to be freely accessible, unless such information is defined as restricted information (either confidential or secret). The access to confidential information of companies can be regulated by adopting a corporate policy declaring certain internal information



OLGA VOROZHBYT IS A SENIOR ASSOCIATE WITH THE KIEV OFFICE OF CHADBOURNE & PARKE LLP. MS. VOROZHBYT RECEIVED LAW DEGREE FROM THE KIEV NATIONAL TARAS SHEVCHENKO UNIVERSITY. MS. VOROZHBYT'S PRACTICE FOCUSES ON LITIGATION AND ARBITRATION



ANDRIY KIRMACH IS AN ASSOCIATE WITH THE KIEV OFFICE OF CHADBOURNE & PARKE LLP. MR. KIRMACH RECEIVED HIS LL.M DEGREE FROM THE NATIONAL UNIVERSITY OF KYIV-MOHYLA ACADEMY

as confidential. This policy can also define rules and procedures of preserving and disclosing such confidential information to third parties. Access to secret information (e.g., state secret information) is regulated by applicable laws and requires a special clearance from state authorities.

The *Data Protection Act*, which comes into legal effect on 1 January 2011, establishes specific requirements for treatment of the personal data of individuals. In particular, the *Data Protection Act* provides that explicit consent of an individual is required for (i) collection and processing of his/her personal information; (ii) granting access to or transferring of personal information of an individual to a third party, etc. Consequently, an individual may reasonably claim that his/her personal information (i) shall not be transferred to a third party; or (ii) shall be erased from a database, especially when there was no consent for collection or transfer of the personal data.

What is Personal Data?

It seems unclear as to what information must be considered personal data within the meaning of the *Data Protection Act*. The *Information Act* provides that basic personal data includes information regarding nationality, education, family status, religion, health status, address, date and place of birth of a particular individual. However, the *Data Protection Act* contains a much broader definition of personal data, stating that "personal data shall be any data (information) about an individual, which individual is identified or could be precisely identified".

The formal reading of provided definition permits considering any information related also to the employment of an individual, e.g., salary, employment benefits, business trips schedule, etc., as the personal data of such individual. Moreover, it can also

be argued that information about the facts of employee's meetings, phone calls, etc., shall be deemed the personal data about such individual and, thus, fall within the framework of the *Data Protection Act*.

There is always a reasonable counter-argument that the discussed information consists of terms of employment or results of an employee's performance. As such, a company is entitled to access and process any such personal information without any limitations as a matter of the company's operational necessity.

That notwithstanding, due to the sensitive nature of personal information and broad definition set out in the *Data Protection Act*, the personal data of an employee needs to be treated with special care.

Access to Personal Data of Employees

Ukrainian laws do not expressly regulate an employer's accessing an employee's personal data, including information stored on a corporate e-mail account or laptop, business telephone records, etc. As a matter of practice, these matters are often regulated by applicable corporate policies, if regulated at all.

A comprehensive corporate policy usually provides that employees must use all corporate resources and devices, including all means of communication, exclusively for the purposes of carrying out employment functions. Such a requirement anticipates that all information processed through corporate devices must always remain open and accessible to the company. This effectively means that any correspondence or calls made by an employee shall not be considered as his/her "personal" communication, but rather the commercial information of the company.

In most internal reviews and investigations, collection and process-

ing of information about an employee (personal data) would require obtaining his/her consent in addition to the acknowledgment of existing corporate policy. In particular, such consent is highly recommended for investigations targeting the personal data of certain employees. At the same time, when personal data is collected incidentally (e.g., together with commercial and financial documents of a company), the risk associated with accessing personal data without the written consent of an employee seems to be remote, especially when such personal data was not processed for the purposes of the investigation and was not further disclosed.

In the event that the company fails to comply with the applicable rules and procedures, it may be precluded from using the revealed data as evidence for the purposes of internal reporting. Additionally, if certain information was collected without due process, the results of the internal investigation may be treated as inadmissible evidence in the courts of Ukraine or other jurisdictions. Furthermore, an employee may claim removal of such information from the company's records and claim damages.

Recommended Actions for Employers

In light of the recently adopted *Data Protection Act*, each company should focus attention to the collection and use of personal data of its employees. It is for the benefit of the company to comply with the *Data Protection Act* and other requirements so that no risks arise from processing and further possible disclosure of employees' personal data for various purposes.

In particular, the following steps could be taken to formalize the collection and processing of the personal data of employees by the company:

1) Enforcement of corporate policies related to use of the company's resources and property (e-mail account, laptop, mobile phone, flash drives, etc.) for business purposes only. Such policies, *inter alia*, should include:

(i) explicit consent of the employee for collection and processing (including transfer to third parties, when needed) of his/her personal data provided to the company at all times;

(ii) clear regulation that all information created, accessed or trans-

ferred through corporate technical devices shall be used for business purposes only, and not for private communication;

(iii) employee's understanding and consent that all information maintained via corporate technical devices can be monitored by the employer, and that an employee shall not expect such information to be treated as private;

(iv) employer's rights to check, collect and process all data (including personal employee's data) located at corporate technical devices at any time, for any reason, and without any additional consent.

2) Employees must acknowledge their consent and understanding of such policies by signing and dating the respective notification document. As a matter of practice, the acknowledgment notices shall be maintained in hard copies, since electronic documentation is largely unregulated in Ukraine and a company may face difficulties proving that a particular employee was aware of the applicable policy. It is also recommended to have the corporate policy available in the Ukrainian language (or in bilingual form).

3) Other company documents, i.e., charter (by-laws), internal regulations, internal labor rules, collective agreement and individual employment agreements, etc., should be maintained in line with applicable policies on personal data and use of corporate technical devices.

4) For collection of the information during internal investigations, it is also recommended that a separate, so-called "document hold", notice be issued to all employees involved. Such notices shall contain explicit instructions to preserve and not to delete certain information, remind employees of their consent to provide personal data to the company and company's right to collect and process any and all data located at corporate technical devices for the purposes of internal investigation.

Following these rather simple procedures would allow the company to ensure compliance with applicable Ukrainian laws. As a result, the company would mitigate potential risks related to the legal standing of evidence collected in the course of internal reviews and investigations and prevent an employee's claims.

Profile

Chadbourne & Parke LLP

Address:

25B Sahaydachnoho Street, 3 Floor,
Kiev, 04070, Ukraine

Tel.: **+380 44 461 7575**

Fax: **+380 44 461 7576**

E-mail: **kyiv@chadbourne.com**

Web-site: **www.chadbourne.com**

Chadbourne & Parke LLP is an international law firm with over 450 attorneys in 13 offices located in New York, Washington, Los Angeles, Mexico City, São Paulo, London, Moscow, St. Petersburg, Warsaw, Kiev, Almaty, Dubai and Beijing. Since its founding in 1902, Chadbourne has been dedicated to providing practical business solutions to a diverse range of clients in virtually all areas of law. Chadbourne is among the leading U.S. law firms in Central and Eastern Europe. Our lawyers not only have in-depth knowledge of the region, but also a significant amount of experience on both complex transactions and day-to-day legal issues that arise for companies doing business in the region, which enables us to anticipate and solve problems in this dynamic legal environment.

Chadbourne has one of the leading Ukrainian law practices. We have a very strong group of Ukrainian and expatriate lawyers with an extensive range of experience in Ukraine, which has worked together as a unified team for more than 17 years. Our Kiev office includes U.S.-, English- and Ukrainian-qualified attorneys. Our partners are consistently ranked among the top lawyers in Ukraine and the Kiev office is recognized by legal directories including Chambers Global, Chambers Europe, IFLR1000, Legal 500 and PLC Which Lawyer as a leading law firm in Ukraine, particularly in the areas of corporate/commercial and banking and finance.

The Kiev office of Chadbourne & Parke LLP provides a full-range of legal services to clients on a variety of matters, including mergers and acquisitions, corporate law, commercial law, banking and finance, dispute resolution, compliance reviews and investigations, corporate finance, securities, real estate, energy, tax, bankruptcy and financial restructuring, employment, insurance, intellectual property, antitrust and others.

Thoroughness, practicality, responsiveness, promptness — these are the principles that guide us in our delivery of services. These are the reasons why our clients keep coming back to us.