

Keenethics

Data Protection Impact Assessment

GDPR focused





11.05.2021

1) General issues

NB! Please, note that parts in italics are direct quotations from the GDPR and other sources

1) General issues.

1. According to the information provided in the Annex 1 to this Assessment by Keenethics LTD (“the Company”) is the software development company that is providing services on the outsource model. The Company is providing its services for different clients and while developing and administering the software products the employees and contractors of the company are inevitably accessing, using and transferring the personal data.
2. According to Article 4 of the GDPR ‘processing’ means *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*. Therefore, even by simply accessing the personal data the Company is processing it, within meaning attributed to this notion by the GDPR let alone by performing the other planned operations, in particular transfer of personal data to sub-processors outside the EU (see § below).
3. As for now, the Company and its contractors are working over two projects within which the personal data is processed, encrypted as ‘Project 1’ and ‘Project 2’. While developing of these projects the Company performs the processing operations of the users of the software products, which are collected by its Clients, who are owners of the software products.
4. Therefore, the Company acts as a Processor within the meaning of the Regulation since as it is laid down in Article 4 of the GDPR it *“determines the purposes and means of the - processing of personal data”*. In performing its activities the Company uses the services of numerous subcontractors, who also access (i.e. process) personal data transferred from the controller with the view to performing the tasks assigned by the Company. They are Private Entrepreneurs, registered under the Ukrainian law and have separate legal and tax status .In such capacity they act as the sub-processors.
5. So, in case of Company, the following data protection chain applies:

Data Subjects:	Data Controller:	Data Processor:	Data Subprocessors:
users of the software products	Clients of the Company, which are owners of the software products	The Company, which provides software development services	The Company’s Contractors, who are working on the projects
			

6. Whilst the Company's main establishment and its sub-processors are located in Ukraine which is not the member state of the EU or the EEA, are located on the territory of Ukraine which is member of neither EU nor EEA. Therefore, the Company's activities, which envisage transfer of the EU citizens and residents personal data to "third countries" within the meaning attributed by the GDPR.
7. The three main questions which should be specially analysed in this case are:
 - a) Whether the Company has a duty to appoint a representative within the European Union?
 - b) Whether the Company effectively implements a requirement to designate a Data Protection Officer?
 - c) Whether the Company effectively implements a requirement to provide a corporate Data Protection Policy?
8. The subject matter of this assessment is to analyse the personal data processing operations performed by the company and to evaluate the current data protection measures, already taken by the Company and to determine what measures are necessary to ensure their full compliance with the GDPR. Two crucial issues in this regard appears to be:
 - a) the transfer of the personal data of the Union residents outside the Union;
 - b) a processing of the information about EU residents and citizens, who are using software products, which are developed by the Company.

2) Obligation to appoint a representative within the European Union.

9. If the GDOR is directly applicable to activities of the **controller**, it might under certain circumstances entail the obligation to designate a controller's representative in the Union. Thus, according to Article 27 of the GDPR "*where Article 3 (2) applies, the controller shall designate in writing a representative in the Union*".
10. Nonetheless the obligation to designate a representative does not apply to processing which is
 - 1) **occasional**,
 - 2) **does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and**
 - 3) **is unlikely to result in a risk to the rights and freedoms of natural persons**, taking into account the nature, context, scope and purposes of the processing.
11. It is to be noted that to be excluded from the scope of the above provision (i.e. released from the obligation to appoint a representative) **all three aforementioned conditions should be met**. The obligation to appoint a representative will be analyzed below through the prism of the types of personal data, which are processed by the Company, which are specified in the para 7.
 - a) When it goes about the **occasional** processing, it can be concluded that the Company matches this condition mainly because the processing of the personal data is not main scope

of Company's business and the services it is providing to its Clients. Thus, processing of the personal data is not taking place **permanently**.

b) The Article 9(1) and 9(2)(f) of the GDPR regulates and provides guarantees concerning the *"processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"*. As we may see from Annexes to this Assessment, the Company is not processing such types of data within the Projects. Thus, it can be assumed that the Company's activities will not fall under the condition of **the large scale processing of special categories of data as referred to in Article 9(1) of GDPR**.

c) To establish whether processing operations within the above projects satisfy **the third condition** envisaged by Article 27 (2) of the GDPR, namely **risk to the rights and freedoms of natural persons** we can again analyze the Information provided by the Company in the Annexes. The conclusions obviously say that no such risk takes place.

12. **Therefore, due to the foregoing analysis it is proposed that the Company is not under the duty to designate a representative in the Union, i.e. in one of the Member States where the data subjects, whose personal data are processed, reside.**

3) Designation of a Data Protection Officer.

13. According to Article 37 (1) of the GDPR the controller and the processor shall designate a data protection officer in any case where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- **the core activities** of the controller or the processor **consist of processing on a large scale of special categories of data pursuant to Article 9** or personal data relating to criminal convictions and offences referred to in Article 10.

14. In case of the Company's business model, the appointment of the DPA additionally allows to bring the sub-processors' data protection measures in conformity with Company's policy and, thus, standardize their approach to this issue.

15. According to the information provided by the Company, they have a person who is acting as a Data Protection Officer on the contract basis and has appropriate professional qualifications and experience to act in this capacity, namely Natalia Vasylechko, Attorney-at-Law.

16. **Therefore, it can be recognized, that Company takes proactive position in this regard and fully complies with the GDPR requirements.**

4) General Data Protection Policy.

17. According to Article 5 (2) of the GDPR *“the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).”* which lays down key principles of data protection.
18. According to Article 32 (1) of the GDPR *“Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk”*.
19. The Recital 78 providing some clarification of the above provisions of the GDPR states that *“The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met”*. It further recommends that *“in order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies”*.
20. According to the information provided by the Company, they have a person who is acting as a Data Protection Officer on the contract basis and has appropriate professional qualifications and experience to act in this capacity, namely Natalia Vasylechko, Attorney-at-Law, contact: natalia@dexis.partners.
21. According to the information provided by the Company, in 2018 they have a person who is acting as a Data Protection Officer on the contract basis and has appropriate professional qualifications and experience to act in this capacity, namely Natalia Vasylechko, Attorney-at-Law, contact: natalia@dexis.partners
22. **Therefore, it can be recognized, that Company takes proactive position in this regard and complies with the GDPR requirements, but there is a need for the review and update of the Data Protection Policy.**

5) Whether the foregoing reflections necessitate change of the Company’s technical and organizational measures.

23. It is to be noted that the appropriateness of technical and organizational measures necessary to ensure an adequate level of security that should be implemented by the company should be determined according to Article 32 of the GDPR *“taking into account the state of the art, the costs of implementation and **the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons**”*.
24. It is to be noted that according to the Recital 75 *“**the risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical***

*beliefs, trade union membership, and **the processing of genetic data, data concerning health** or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or **where processing involves a large amount of personal data and affects a large number of data subjects**".*

25. In the case at hand the company processes personal data that might fall into the above categories (see text in bold). The amount of data processed is not huge and the data itself, do not pose any serious risk to data subjects even if unlawfully revealed. What is important is that the personal data processed doesn't pose any interest from a financial or any other point of view which reduces the potential interest in their unlawful disclosure. Therefore, the risk for the rights and freedoms of natural persons presented by the processing of the above data can be considered as low.
26. Referring to the aforementioned reflection if the additional precautions listed below are implemented by the Company, its organisational and technical level of data security might be qualified as absolutely sufficient. Such measures should include the following options:
- Measures concerning organization of data protection security include:
- a) The update and a regular (at least annual) review of the Data Protection policy, approved by senior management and disseminated among its Personnel.
 - b) Ensuring that all users access the company systems with a unique identifier (user ID) and shared accounts are prohibited. Working session are automatically terminated off, if the account is not used for a limited period of minutes. "Autorun" function for external devices is deactivated.
 - c) Establishing a password verification policy that prohibits the sharing of passwords and requires passwords to be changed on a regular basis and default passwords to be altered after the first connection. All passwords must fulfil defined minimum requirements and are stored in encrypted form. Each computer has a password-protected screensaver. "CAPTCHA" and login challenge to verify the identity is used.
 - d) Having a thorough procedure to deactivate users and their access when a user leaves the company or a function or the appropriate master service contract is terminated.
 - e) Restricting Personnel access to files and programs on a "need-to-know" basis.
 - f) Using up-to-date and regularly updated anti-virus software, on all appropriate computers and servers or computers and servers with secured by default operating systems;
 - g) Protecting corporate e-mail server by anti-virus and/or mailing services which provide appropriate security measures;
 - h) Providing a Controller with a list of individual (natural person) subcontractors who are used to help it provide the services and regular informing of Controller about any changes in this list
 - j) Not using cloud services without preliminary profound analysis of its conditions of use and security measures;
 - i) Conducting periodical and external audits of its security

6) Final remarks.

By this Assessment we prove that the Company takes reasonable steps to ensure that Personnel are aware of and comply with the technical and organizational measures set forth above. The Company may change these measures from time to time by replacing individual measures by new measures that serve the same purpose or deal with the same risks without materially diminishing the security level. **We can conclude that the Company can be considered as a GDPR compliant.**

**Ivan Horodyskyy,
Attorney-at-Law,
Managing Partner,
Dexis Partners Law Firm**



PROJECT 1

1. Please describe the database (project):

Project 1 is a biography writing service which helps people write books about their lives. Bookmaker is the platform that is used to enable the whole book production process: storytellers, writers, and editors communicate here and collaborate on creating the book.

2. The company carries out:

- 1) the development of the database and the processing of personal data in the test mode;
- 2) database administration and ongoing processing of personal data;

3. Processing of which categories of personal data is carried out in the database/within the project (in several sentences, types of personal data which are processed):

- First name and last name, address, email, password, phone number.
- Life stories information, personal photos.

4. The personal data of what subjects is being processed (briefly, for example: purchasers, users of software developed by the company, etc.):

- Clients of the Project 1 service (storytellers) and providers of the Project 1 service (writers, editors)

5. Are personal data transferred to third parties (to the other companies, private individuals, etc.):

2) No;

6. For what purpose, personal data in the database/within the project is being processed (please describe in 1-2 sentences, for example: processing of data on the purchase of Internet shop users, etc.):

- Data is processed in order to organize and manage communication between service clients and providers, to enable the process of book production

7. The personal data is processed with the purpose of:

- offering services or goods to customers in the EU;

8. How often personal data in the database/within the project is processed?

1) Regularly;*

Other (commentary):

9. In what volumes is the personal data of citizens of EU Member States is processed in the database/within the project?

1) large (thousands +)

10. Are records of operations (logs) with files that contain personal data?

1) Yes;

10.1. If so, what information, in this case, is fixed in the logs:

o the start and end time of the operation, its duration;

o data about the file that was viewed;

o data about the browser from which the operation was performed;

11. Who can access the database and files that contain personal data:

1) Only those persons/employees who need access to personal data in accordance with their responsibilities?

12. Whether the level of access to personal data in the database is differentiated (for example, "administrator" - editing, deleting and granting access, "editor" - editing and viewing, "user" - viewing):

1) Yes;

ANNEX 3

PROJECT 2

1. Please describe the database (project):

At Project 1, we specialize in creating a strong culture where everyone sees themselves as a leader. We believe that leadership develops in many different contexts, starting within yourself! Reflecting on personal values, seeking other perspectives, and activating yourself are all necessary for cultivating a better sense of self, which will allow you to influence others in a positive, shared direction.

2. The company carries out:

The development of the database and the processing of personal data in the test mode;

3. Processing of which categories of personal data is carried out in the database/within the project (in several sentences, types of personal data which are processed):

1. email, name
2. Values, strengths and feedbacks of the users

4. The personal data of what subjects is being processed (briefly, for example: purchasers, users of software developed by the company, etc.):

1. Project 2 clients

5. Are personal data transferred to third parties (to the other companies, private individuals, etc.):

No;

6. For what purpose, personal data in the database/within the project is being processed (please describe in 1-2 sentences, for example: processing of data on the purchase of Internet shop users, etc.):

1. Analyze feedbacks and personal and company development goals

7. Is personal data processed with the purpose of:

- offering services or goods to customers in the EU;

8. How often personal data in the database/within the project is processed?

1) Rarely.

9. In what volumes is the personal data of citizens of EU Member States is processed in the database/within the project?

WARNING! The information contained in this file is intended for use by only such persons who are entitled to use it from Dexis Partners. Do not copy or redirect this file without the express permission of Dexis Partners. When you have finished working with the file, please, remove it completely from your computer system.

1) large (thousands +)

10. Are records of operations (logs) with files that contain personal data?

1) Yes;

10.1. If so, what information, in this case, is fixed in the logs:

- o the start and end time of the operation, its duration;
- o IP address of the user;
- o data about the file that was viewed;

11. Who can access the database and files that contain personal data:

3) Only those persons/employees who need access to personal data in accordance with their responsibilities?

12. Whether the level of access to personal data in the database is differentiated (for example, "administrator" - editing, deleting, and granting access, "editor" - editing and viewing, "user" - viewing):

2) Partially (describe in the commentary);

Other (commentary): Administrator Role - can see and share to the customer company by request.

User – can see its own personal data