LEWIATAN

Polish Confederation Lewiatan

CONTRIBUTION TO THE DEBATE ON EU PERSONAL DATA PROTECTION REFORM

Warsaw, February 2015

HUMAN CAPITAL
NATIONAL COHESION STRATEGY

LEWIATAN

EUROPEAN UNION
EUROPEAN
SOCIAL FUND

Publication co-funded by the European Union under the European Social Fund

Table of contents

Part 1.

Economic consequences for SME of the EU regulation on the protection of personal data

Dear Sir/Madam,

After two years of discussion, 4000 submitted amendments and a stormy public debate the committee of the European Parliament LIBE adopted a report of the draft Regulation on the protection of personal data[1]. The adopted position expressed the consent of members of the Parliament as to the economic and social value of personal data and therefore their need to be properly protected.

Fully supporting this approach, the Polish Confederation Lewiatan and the Chamber of Digital Economy decided to verify how the rules proposed by the Parliament would work in practice, i.e. how they would affect everyday life of the average entrepreneur who while conducting business activity processes data on a small or moderate scale. Our aim was to check whether the obligations the controller will have to fulfill are proportional and if limitations in data processing shall not hinder the implementation of their legitimate interests. Finally, we tried to estimate what will be the associated costs.

To get a full picture, we chose very different activity profiles. We analyzed the report of the draft Regulation for the obligations that would have to be met by an entrepreneur selling their products via the Internet (online bookstore), an entrepreneur providing services outside the digital environment (beauty salon) and a controller leading a non-profit activity (MEP).

The conclusions of this analysis indicate that the rules proposed by LIBE are based on incorrect assumptions. The imposed obligations are insufficiently differenciated depending on the nature and scale of the data processing and potential risks. Even those controllers who process data on the minimum level will have to comply with the extensive list of obligations designed for the most advanced and risky cases of data processing. They will also bear the costs resulting from the necessity to ensure compliance with the required organisational solutions. **According to our analysis, the total costs of the documentation requirements under the Regulation, in the first two years of conducting business activity by each of the analysed entrepreneurs, can be estimated at not less than PLN 66 600 + VAT**. This sum covers only the costs of drafting documents and informative clauses, including the costs associated with legal services and services provided by the data protection officer. It does not include the cost of activities needed for the actual protection of personal data against loss and damage. What seems to be alarming is the fact that the cost of implementing the new law for entrepreneurs performing operations on personal data on a minimum and socially harmless level will be nine times as high as it was before.

It is true that companies have already borne some costs associated with ensuring compliance with the rules which often exceed the aforementioned amounts. However, a vital problem illustrated in the attached material is that these costs will be borne by almost everyone in the event of the adoption of the LIBE version of the Regulation.

The attached material is designed to help eliminate unnecessary burdens. According to the Polish Confederation Lewiatan and e-Chamber, the Regulation should not be adopted until all the provisions generating unreasonable costs will be removed. Otherwise, the chance to exploit the potential of the Internet economy for the creation and development of innovative and competitive businesses in Poland and the European Union will be lost.

On behalf of the Polish Confederation Lewiatan:

Henryka Bochniarz
President

On behalf of the Chamber of Digital Economy:

Grzegorz Wójcik
Member of the Board

1 Analysis of the obligations included in LIBE Report on 20th October 2013

About Polish Confederation Lewiatan and Chamber of Digital Economy

POLISH CONFEDERATION
LEWIATAN

Polish Confederation Lewiatan was established in January 1999 as a nation-wide representation of employers to the state and trade unions. Today it is an organization of 62 sectoral and regional associations of private employers and 25 individual members. In total about 3 900 companies employing over 900 000 workers are represented.

Lewiatan's working group on data protection regulation was established at the beginning of 2012, after the presentation of the proposal by the European Commission. It is composed of companies from many sectors, such as e-commerce, banking, retail, ICT, insurance, and marketing. It includes, of course, SMEs and companies of Polish origin.

Lewiatan has been very active on data protection reform, both at national and EU level. It aims to ensure that data protection rules are proportionate and enable the pursuit of legitimate business activity. We believe that for the sake of the Polish and European economies, a great deal of cost and administrative burden for business should be eliminated form the proposal.

e-COMMERCE POLSKA
IZBA GOSPODARKI ELEKTRONICZNEJ

The Chamber of the Digital Economy (e-Chamber) is a nation-wide, non-profit Polish industry organisation, representing a wide range of companies that use Internet and digital services to grow their business, in particular the leaders and SMEs of the e-commerce sector including e-retailers, online payment solution providers, online IT services, and e-commerce logistics operators gathered around its core project „e-Commerce Polska".

The primary goal of the organisation is to facilitate market growth through cooperation, exchange of know-how, education and strong and effective representation of the industry interests in dialogue with both government and non- governmental institutions.

The companies and partners engaged in e-Chamber deeply believe in the development of European economy in various industries through the use of technological innovation, information and communication technologies (ICT), particularly the Internet, and practical applications of digital information exchange in business.

MODEL No. 1

ONLINE BOOKSTORE

Description of the activity

An individual who conducts business activity plans to open an online bookstore. The offer shall include: (1) mail order sale of books and (2) providing access to e-books on the website or via an application that allows the use of the bookstore's resources through such devices as mobile phones and tablets.

The owner of the bookstore (hereinafter referred to as the Bookstore) will lead marketing limited to the newsletter containing offers tailored to the interests of the customer.

The Bookstore shall process personal data of its: (1) customers, i.e. people who made a purchase and whose data were necessary to arrange shipment, and (2) people interested in the Bookstore's offer.

The Bookstore shall cooperate in terms of common business services with a number of companies, e.g. a web hosting provider, courier company, software supplier. Since the Bookstore will offer the customers a mobile application for tablets and mobile phones, it will have to use services of the two providers of operating systems that create the working environment for such applications, i.e. Google (Android system) and Apple. These entities will process personal data whose controller shall be the Bookstore on the basis of entrustment.

The Bookstore decided to reduce the number of personal data operations to a minimum in order to minimise the extent of its obligations arising from the provisions on the personal data protection.

Consequences in terms of personal data protection

GENERAL OBLIGATIONS WITH REGARD TO DATA PROCESSING[2]

Currently with the start of its business activity the Bookstore has to prepare two documents: Data security policy and Instruction for managing the IT system. These documents describe files of personal data and the method of their protection. The Bookstore should also conclude simple entrustment agreements indicating the purpose and scope of data processing. The agreements should be concluded in writing but non fulfilment of this requirement willnot make the agreement void.

After the implementation of the LIBE version of the Regulation, much more comprehensive documentation will be required. The Bookstore will be obliged to:

1. draft concise, transparent, clear and easily accessible policies with regard to the processing of personal data and for the protection of rights of data subjects (Art. 11 (1) LIBE). The content of the LIBE document suggests that the policies shall be published (made easily accessible) by the Bookstore;
2. adopt and implement appropriate policies and implement appropriate and demonstrable technical and organisational measures (Art. 22 (1) LIBE) accompanied by the compliance policies that shall be reviewed every two years (Art. 22 (1a) LIBE). The Bookstore will need to be able to demonstrate the adequacy and effectiveness of the taken measures;
3. draft documentation necessary to fulfill the requirements laid down in the Regulation (Art. 28 (1) LIBE). All the activities related to the processing of data (e.g. installation of anti-virus or cryptographic software) shall be registered and documented by the Bookstore;
4. carry out the risk analysis (an obligation arises from exceeding the limit of 5,000 data subjects, which in the digital environment is low ceiling – Art. 32a (2) (b) LIBE). The analysis shall be documented in writing and reviewed once a year (Art. 32a (4);
5. carry out data protection impact assessment (Art. 33 (1) in conjunction with Art. 32a (3) LIBE);
6. hire (under a contract) a data protection officer (Art. 32a (3) (b) LIBE) – this obligation applies to a controller who will collect at least 5,000 data subjects, which is a small number for an online bookstore.
7. introduce measures verifying the age of users entering their e-mail addresses for the purpose of newsletter e- mailing, and – in the case of users younger than 13 years – mechanisms for obtaining the consent of parents/legal guardians.

IN ADDITION, AFTER TWO YEARS OF THE ACTIVITY THE BOOKSTORE SHALL:

1. review the applied policies (Art. 22 (1) LIBE); the review shall be documented (Art. 28 (1) LIBE);
2. carry out and document a compliance review (Art. 33a LIBE);
3. conclude specific entrustment agreements of the processing of personal data in the case of allowing access to personal data to outside providers (for example, a company providing web hosting service).

All entrustment agreements shall be documented in writing (Art. 26 (3) LIBE) – an entrustment agreement concluded in the electronic version shall not meet the requirements.

It is difficult to imagine that providers of digital environments for mobile applications (i.e. Google and Apple) conclude entrustment agreements in writing with small businesses such as the Bookstore. Even if such agreements are concluded (in any form), in practice the Bookstore will not have any possibility to negotiate their content. In the case of any deficiencies in this respect, financial penalties could be imposed and a responsible entity shall be the controller, i.e. the Bookstore.

2 Analysis of the obligations included in LIBE Report on 20th October 2013.

THE ACQUISITION OF PERSONAL DATA

When the customer of the Bookstore gives any of their personal data, e.g. e-mail address necessary for newsletter e- mailing or correspondence data – for the shipment purposes, the Bookstore will have to publish on the website in the graphic and textual form the following information:

1. whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;
2. whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;
3. whether personal data are processed for purposes other than the purposes for which they were collected;
4. whether personal data are disseminated to commercial third parties;
5. whether personal data are sold or rented out;
6. whether personal data are retained in encrypted form (Art. 13a LIBE).

For all of the above questions, in the case of the Bookstore, the answer is negative. The Bookstore is not particularly obliged to encrypt the retained data. Data encryption involves the purchase of appropriate software and is not

necessary in the case of the Bookstore. The Bookstore, however, shall disclose that it does not encrypt the retained data, which could undermine confidence of the Bookstore's potential customers. The Bookstore, though, shall process and protect personal data in accordance with the rules of the Regulation.

Provided the Bookstore wished to assign receivables to debt collection companies, which is a common practice in the case of small claims, the Bookstore would have to inform the customer about this fact (3). This would be another factor discouraging customers from the Bookstore's services.

THEN, THE BOOKSTORE SHALL PRESENT TO THE CUSTOMERS AND DISPLAY THE FOLLOWING INFORMATION:

1. the identity and the contact details of the controller;
2. the purposes of the processing for which the personal data are intended;
3. the right to request access to and rectif ication or erasure of the personal data and to object to the processing of such personal data, or to obtain data;
4. the recipients or categories of recipients of the personal data;
   The Bookstore will be also obliged to disclose a range of new information that has not yet been published. In particular it must include information about:
5. the identity and the contact details of the data protection officer;
6. the security of the processing of personal data, including the contract terms under which data will be processed, and the method of data processing, or how they meet requirements specified in Art. 6 (1) (f) LIBE, in the case of the newsletter e-mailing;
7. the period for which the personal data will be stored, or if this is not possible, the criteria used to det ermine this period;
8. the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
9. the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;
10. the logic involved in any automated processing;
11. whether personal data were submitted to public authorities during the last consecutive 12-month period;
12. any further information which is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected or processed, in particular the existence of certain processing activities for which a personal data impact assessment has indicated that there may be a high risk.
    [after: Art. 14 LIBE]

Publishing information on the safety of data processing, see point 6) above, it is not required for the protection of the rights of the Bookstore's customers. On the contrary, the implementation of this obligation may lead to the publicatio n of information, the disclosure of which would reduce the level of data security.

Automated processing referred to in point 10) includes any processing of data in information systems (e.g. on a server), whereas the logic is used by any computer program. The Bookstore, thus, shall specify all, even the most obvious software features processing personal data.

The information referred to in point 11) shall be submitted even when the Bookstore will pursue claims in court proceedings. Filing a lawsuit involves providing personal data to public authorities by the Bookstore.

Although the above set of obligations is really extensive, it is not restricted, and in practice the Bookstore may be required to submit additional information referred to in point 12).

The customer shall become familiar with the above information before giving the Bookstore their personal data. It will not be sufficient for the Bookstore to indicate a link to a subpage containing this information. The information need to be presented in such a way that the customer could read it before submitting data. A question remains how to compose and present such a large amount of information so that it can be transparent to the customer who enters their personal data, for example, by using the application on a mobile phone or tablet.

PROFILING AND SENSITIVE DATA

1. The Bookstore plans to adjust the offer to the customers' expectations by presenting it on the home page, on the customer profile and by sending information about the offer via newsletter. For example, a customer who browsed some books in the „detective fiction", will receive in the newsletter information about new detective stories on the Bookstore's offer. The adjustment of the Bookstore's offer to the customer's interests requires providing the customer with additional information about profiling, irrespective of whether the Bookstore will process the customer's personal data or the data will be pseudonymised (Art. 20 LIBE).
2. The Bookstore, however, should not make offers based on profiling if the browsed titles included offers of the Catholic press, books on religious, political or philosophical subjects, women's literature or books about certain diseases and health problems. Such offers may be considered as the creation of profiles based solely on sensitive data and may consequently lead to the infringement of provisions on profiling and sensitive data protection (see Art. 9 and 20 (3) LIBE).
3. Since gender identity is considered among sensitive data, the way the Bookstore addresses correspondence to a given customer may be prohibited from processing of sensitive data (Art. 9 (1) LIBE).

PROCESSING OF PERSONAL DATA OF A CHILD AND CONSENT TO THE PROCESSING OF DATA

1. In order to offer books to children and young people, the Bookstore shall verify if consent to purchase a book by a child was given by their guardian (Art. 8 (1) LIBE). The Bookstore, however, will not be able to verify such consent in any way. A checkbox with a relevant statement shall not be sufficient. Since the lack of complianc e with this obligation may involve a financial penalty (Art. 79 LIBE), the Bookstore will have to give up this type of sale.
2. E-mail addresses are, as a rule, personal data. Processing them for the purpose of newsletter e-mailing containing promotional material of other entities shall not be allowed without the consent of the person sending the data. Since the consent to the processing of data must be explicit (Art. 4 (8) LIBE), the mere sending of an e-mail address shall not be deemed as consent. A person interested in receiving a newsletter will need to select an additional checkbox, which will express consent to data processing for the purpose of newsletter e-mailing.

3. The Bookstore shall not offer the customers, who will agree to receive commercial information, any additional free services. It is because the consent to the processing of personal data shall not be a condition to provide a service (Art. 7 (4) LIBE).

ORDER ON BEHALF OF THE THIRD PARTY

If the customer places an order and gives details of a third party who is going to be sent a book (e.g. as a gift), the basis of data processing shall be a legitimate interest of the controller (Art. (1) (f) LIBE). The third party may, however, at any time object to the processing, and the Bookstore will be obliged to delete the data irrespective of whether they may be necessary to prove that the service has been performed by the Bookstore (Art. 19 (2) LIBE).

DEBT COLLECTION. TRANSFER OF PERSONAL DATA TO A DEBT COLLECTION COMPANY

The provisions of the Regulation do not give a clear answer whether there is a legal basis to conduct debt collection by the Bookstore after it has performed the agreement. It seems that the Bookstore shall not pass debtors' personal data to a collection company, which shall acquire from the Bookstore debt claims arising from the goods supplied and services rendered, and it shall assert these claims on its own behalf (see Art. 5 (b) LIBE). The debt recovery process may be significantly hindered since the Bookstore does not have the resources to support it.

CHANGING THE PURPOSE OF THE PROCESSING

The Bookstore shall not draw up its own statistics on the sales process, for example, analysing how customers make purchases or from which regions of the country of the EU orders are made. For instance, the Excel table containing only order prices and delivery locations will contain pseudonymised data treated in this respect in the same way as personal data (Art. 20 (1) LIBE). Drafting the table shall involve an unacceptable change of the purpose of personal data processing.

PROCESSING OF PERSONAL DATA FOR DOCUMENTATION PURPOSES

The Bookstore shall purchase and implement software that will enable the erasure of personal data after the completion of the processing (Art. 17 (8b) (b) LIBE).

PENALTIES

1. Infringement of any of the above provisions of the Regulation shall involve the imposition of a financial penalty on the Bookstore (Art. 79 LIBE). Penalties may be imposed on the performance of all obligations under the Regulation, even those whose performance may raise practical concerns (e.g. regarding the protection of personal data of a child), and those whose implementation does not directly affect the degree of the protection of data subjects' rights (e.g. documentation requirements).
2. Financial penalties may be imposed irrespective of the degree of responsibility (Art. 79 LIBE). Limitation of financial liability of the Bookstore to intentional or negligent incompliance shall apply only in the case of possession of a valid European Data Protection Seal – Art. 79 (2b). In order to obtain such guarantee, the Bookstore will need to incur additional costs of the audit – Art. 39 (2a).

COSTS

In order to to meet the above obligations concerning implementation of the provisions of the Regulation, the Bookstore shall bear significant costs of the preparation and maintenance of the required documentation, as well as organisational measures required by the Regulation.

The costs have been calculated with reference to the current market rates, need of the services provided by specialised consulting companies and serious legal and financial risk incriminating both the Bookstore and Bookstore's service provider (e.g. the data protection officer), which always influences an increase in prices of services.

Given the need to use the services of a professional consulting company (implementation of the obligations requires specialist legal and often also technical knowledge, which the Bookstore does not have), the amount of the expenditure in question can be estimated as follows:

1. drafting policies with regard to the processing of personal data and the protection of data subjects' rights (Art. 11 (1) LIBE) – PLN 6,000 net
2. preparation of informative clauses (Art. 13a and 14 LIBE) – PLN 600 net
3. implementation of compliance policies (Art. 22 (1a) LIBE) – a minimum of PLN 6,000 net
4. review and documentation of the risk analysis (Art. 32a (4) LIBE) – a minimum of PLN 6,000 net
5. arrying out data protection impact assessment (Art. 33 (1) in conjunction with Art. 32a (3) LIBE) – a minimum of PLN 6,000 net
6. preparation of written entrustment agreements on the processing of personal data for at least two entities (web hosting and software providers) – PLN 1,500 net.

The Bookstore will need to conclude an agreement with a data protection officer (Art. 32a (3) (b) LIBE). The agreement shall be concluded for a specified period of time. The cost of such fixed service can be estimated (given the minimum amount of the processed data by the Bookstore) at about PLN 1,500 net per month, that is **PLN 18,000 net per year**.

Every year, the Bookstore shall bear the cost of the review and documentation of the risk analysis (Art. 32a (4) LIBE). This procedure will be of the routine nature and its cost can be estimated at about PLN 1,500 net.

After two years of operation, the Bookstore shall bear the costs necessary for the acquisition of the following services:

1. implementation and documentation of the review of applied policies (Art. 22 (1) LIBE); – PLN 1,500 net;
2. implementation and documentation of the compliance review (Art. 33a LIBE) – PLN 1,500 net.

The total costs of the documentation requirements under the Regulation in the first two years of the Bookstore's business activity can be estimated at not less than PLN 66 600 + VAT.

This above calculation has been based on the knowledge of legal services' costs on the Polish market.

This sum covers only the costs of drafting and execution of documents and informative clauses, including the costs associated with legal services and services provided by the data protection officer.

The above estimate does not include the cost of activities necessary for the actual protection of personal data against loss and damage.

The estimate omits, in particular, the cost of purchasing the software for data protection, including anti-virus or cryptographic software, the acquisition costs of web hosting services on properly secured servers, backup costs, and finally, costs of physical security measures that should be introduced in the Bookstore's seat.

MODEL No. 2

MEMBER OF THE EUROPEAN PARLIAMENT

Description of the activity

The Member of the European Parliament (hereinafter referred to as the MEP) within the activities of his or her parliamentary office maintains a website where its users may order newsletter e-mailing. E-mail addresses of the newsletter's recipients are collected in the e-mail database.

The MEP on his or her own behalf also organises competitions where the prize is an internship in the parliamentary office or a visit to the European Parliament. The organisation of competitions requires collecting personal data of their participants (name, e-mail address, correspondence address).

The MEP organises visits to the European Parliament, which involves receiving from schools and other cooperating organisations lists of participants of the tour. The MEP, as the organiser, passes those lists to the entities which on the MEP's behalf provide services necessary to coordinate the visit (e.g. transport services).

The MEP is considering the possibility to use, in some cases, the collected personal data, to inform about his or her activity, in particular to inform about organised conferences and activities related to the next European Parliament election campaign.

The MEP receives correspondence in which senders describe their problems and ask for intervention in specific cases. The content of the letters often reveals their political views or – if asking for help – data on their financial situation, health status, etc. Thus, these data are often sensitive. Correspondence is printed and stored in the records maintained by the staff of the parliamentary office for the purpose of settling the case. The registry of cases containing, among other things, personal data of the senders are kept in an electronic Excel format in the MEP's office.

Consequences in terms of personal data protection[3]

GENERAL OBLIGATIONS WITH REGARD TO DATA PROCESSING

Currently the MEP has to prepare two documents: Data security policy and Instruction for managing the IT system. These documents describe files of personal data and the method of their protection. The MEP should also conclude simple entrustment agreements indicating the purpose and scope of data processing. The agreements should be concluded in writing but non fulfilment of this requirement will not make the agreement void.

After the implementation of the LIBE version of the Regulation, much more comprehensive documentation will be required. The MEP will be obliged to:

3. draft concise, transparent, clear and easily accessible policies with regard to the processing of personal data and for the protection of rights of data subjects (Art. 11 (1) LIBE). The content of the LIBE document suggests that the policies shall be published;
4. adopt and implement appropriate policies and implement appropriate and demonstrable technical and organisational measures (Art. 22 (1) LIBE) accompanied by the compliance policies that shall be reviewed every two years (Art. 22 (1a) LIBE). The MEP will need to be able to demonstrate the adequacy and effectiveness of the taken measures;
5. draft documentation necessary to fulfill the requirements laid down in the Regulation (Art. 28 (1) LIBE) – the modalities of the implementation of the right to be forgotten, the right to object etc. All the activities related to the processing of data (e.g. installation of anti-virus or cryptographic software) shall be registered and documented by the parliamentary office;
6. carry out the risk analysis (an obligation arises from exceeding the limit of 5,000 data subjects – Art. 32a (2) (b) LIBE). The analysis shall be documented in writing and reviewed once a year (Art. 32a (4);
7. carry out data protection impact assessment (Art. 33 (1) in conjunction with Art. 32a (3) LIBE);

IN ADDITION, AFTER TWO YEARS OF THE ACTIVITY THE MEP SHALL:

1. review the applied policies (Art. 22 (1) LIBE); the review shall be documented (Art. 28 (1) LIBE);
2. carry out and document a compliance review (Art. 33a LIBE);
3. In the case of allowing access to personal data to outside providers of the services (for example, a web hosting company, a company organising transport of participants of visits to the European Parliament), the MEP shall conclude specific entrustment agreements of the processing of personal data. All entrustment agreements shall be documented in writing (Art. 26 (3) LIBE) – an entrustment agreement concluded in the electronic version shall not meet the requirements.
4. introduce measures verifying the age of users entering their e-mail addresses for the purpose of newsletter e- mailing, and – in the case of users younger than 13 years – mechanisms for obtaining the consent of parents/legal guardians.

NEWSLETTER

E-mail addresses are, as a rule, personal data. Thus, when a person interested in receiving newsletter e-mailing from the MEP gives their e-mail address, they would accept sharing their personal data. Before receiving the data, the MEP will be obliged to publish on the website in the graphic and textual form the following information:

1. whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;
2. whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;
3. whether personal data are processed for purposes other than the purposes for which they were collected;
4. whether personal data are disseminated to commercial third parties;

3 On the assumption that the Regulation shall apply to the EU institutions

5. whether personal data are sold or rented out;
6. whether personal data are retained in encrypted form. (Art. 13a LIBE)

For all of the above questions, in the case of the MEP, the answer, as a rule, should be negative. Provided the MEP does not encrypt data or makes reasonable use of data for other legitimate interests, he or she shall indicate failure to comply with this obligation.

THEN, ON THE NEWSLETTER ORDER FORM, BEFORE GIVING PERSONAL DATA, THE MEP SHALL DISPLAY THE FOLLOWING INFORMATION:

1. the identity and the contact details of the controller;
2. the purposes of the processing for which the personal data are intended;
3. the right to request access to and rectification or erasure of the personal data and to object to the processing of such personal data, or to obtain data;
4. the recipients or categories of recipients of the personal data;

The MEP will also be obliged to disclose a range of new information that has not yet been published. In particular it must include information about:

5. the security of the processing of personal data, including the contract terms under which data will be processed, and the method of data processing, or how they meet requirements specified in Art. 6 (1) (f) LIBE;
6. the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
7. the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
8. the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;
9. the logic involved in any automated processing;
10. whether personal data were submitted to public authorities during the last consecutive 12-month period;
11. any further information which is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected or processed, in particular the existence of certain processing activities for which a personal data impact assessment has indicated that there may be a high risk.
    [after: Art. 14 LIBE]

Publishing information on the safety of data processing, see point 6) above, it is not required for the protection of the rights of data subjects. On the contrary, the implementation of this obligation may lead to the publication of information, the disclosure of which would reduce the level of data security (e.g. information on data security measures).

Automated processing referred to in point 10) includes any processing of data in information systems (e.g. on a server), whereas the logic is used by any computer program. The MEP, thus, shall specify all, even the most obvious software features processing personal data.

E-mail addresses are, as a rule, personal data. Processing them for the purpose of newsletter e-mailing containing promotional material of other entities (e.g. the MEP's political party) shall not be allowed without the consent of the person sending the data. Since the consent to the processing of data must be explicit (Art. 4 (8) LIBE), the mere sending of an e-mail address shall not be deemed as consent. A person interested in receiving a newsletter will need to select an additional checkbox, which will express consent to data processing for the purpose of newsletter e- mailing.

ORGANISATION OF THE COMPETITION

1. The MEP shall be obliged to present the contestants most of the information described above.
2. A competition, in many cases, is not an agreement but has the nature of a public promise. Therefore, in order to organise a competition, the MEP shall process personal data for the legitimate interests pursued by the controller (Art. 6 (1) (f) LIBE). However, the participant shall at any time (e.g. after receiving the award) object to the processing of their personal data. In this case, the MEP should carry out the erasure of these data without delay (Art. 19 (2) LIBE). The obligation of data erasure is unconditional. The MEP shall lose the right to process personal data, for instance, for purposes of proof to document the progress of the competition or to publish the results of the competition. In order to settle the funds spent on the organisation of the competition, the MEP shall not process data of the participant who objected to it.

ORGANISATION OF VISITS TO THE EUROPEAN PARLIAMENT

1. The MEP as the organiser of visits to the European Parliament shall be the controller of the participants. However, the MEP shall not normally conclude appropriate agreements with the participants of visits. The participants will often be represented by the entities cooperating with the MEP (schools, associations, political parties). After receiving lists of participants of the visit, the MEP shall provide them without delay with extensive information referred to above.
2. The MEP will enable participation in the visit based the processing of data on the grounds of the legitimate interests pursued by the controller (Art. 6 (1) (f) LIBE). In the case of the adoption of such legal basis, the processing of data shall not be possible after the participant's objection. The MEP may receive consent to the processing of personal data from the participant of the visit. Such consent, however, will have to be obtained directly from each participant of the tour, in a written or electronic form. The participation in a visit to the European Parliament that suggests the participant's consent to the processing of their personal data shall not be sufficient. The MEP shall be obliged to document the fact of obtaining such consent from the data subject (Art. 7 (1) LIBE).

SENDING INFORMATION ABOUT THE MEP'S ACTIVITIES

1. A MEP shall not send information and notices on his or her own activities and other projects to those who have entered their personal data in relation to the organisation of visits and competitions, even if according to the MEP, these persons could be directly interested in receiving such information (Art. 5 (b) LIBE).
2. The MEP shall not transfer the collected data to other entities, such as the MEP's political party, for the purpose of promotion (marketing) of the party. This activity would go beyond the purpose of the processing of data by the MEP (Art. 5 (b) LIBE).

PUBLIC SERVICE

1. If the content of the correspondence from the citizens contains sensitive data, the MEP – wishing to settle a given case – shall address the citizen a letter asking to be sent explicit consent necessary for the sensitive data processing for the purpose of settling the case. The MEP shall not indicate any other legal basis for data processing, even if the data were processed in the interest of the person who gave them and the MEP only wished to reply to the received correspondence (Art. 9 (2) LIBE).
2. The MEP's office shall not prepare statistics of the settled cases (e.g. in order to summarise the locations of the citizens reporting the cases). The processing of data for statistical purposes is, thus, limited to statistical research (Art. 83 LIBE).
3. The MEP shall purchase and implement appropriate software that will ensure the erasure of personal data after the completion of the processing (Art. 17 (8b) LIBE).

MODEL No. 3

BEAUTY SALON

Description of the activity

A graduate of a cosmetology school (hereinafter reffered to as the Beautician) would like to open her own beauty salon. As part of her business activity she will process data of her clients. Because of the need to ensure safety (exclusion of an allergic reaction, contraindications), before performing some treatments by the Beautician, the client will have to complete the questionnaire on health status. Therefore, the processed data of her clients will also contain sensitive data. The data are retained in the client's documentation even after the treatment, for the purposes of possible complaints and for reasons of the client's safety.

In order to promote the salon, the Beautician will include in the questionnaire on health status a consent clause for the processing of personal data for marketing purposes. That will enable the Beautician to inform her existing clients about promotions.

The Beautician will use the services of a marketing company in order to gain new clients. For this purpose, she will purchase a database (containing over 5,000 records) and will formally become its controller. The marketing company that will sell (make accessible) the database and will be responsible for the promotion of the salon will act as the processor.

Consequences in terms of personal data protection

GENERAL OBLIGATIONS WITH REGARD TO DATA PROCESSING[4]

Currently with the start of its business activity the Beautician has to prepare two documents: Data security policy and Instruction for managing the IT system. These documents describe files of personal data and the metho d of their protection.

4 Analysis of the obligations included in LIBE Report on 20th October 2013

After the implementation of the Regulation, much more comprehensive documentation will be required. The Beautician will be obliged to:

1. draft concise, transparent, clear and easily accessible policies with regard to the processing of personal data and for the protection of rights of data subjects (Art. 11 (1) LIBE). They will be much more extensive than today. Since they shall be easily accessible, they should be posted on the website and most probably printed and made available in the salon.
2. adopt and implement appropriate policies and implement appropriate and demonstrable technical and organisational measures (Art. 22 (1) LIBE) accompanied by the compliance policies that shall be reviewed every two years (Art. 22 (1a) LIBE). The Beautician will need to be able to demonstrate the adequacy and effectiveness of the taken measures;
3. draft documentation necessary to fulfill the requirements laid down in the Regulation (Art. 28 (1) LIBE).
4. carry out the risk analysis (it seems that due to the processing of sensitive data, a breach of data security could adversely affect the privacy of data subjects, Art. 32a (2) (g) LIBE). The analysis shall be documented in writing and reviewed once a year (Art. 32a (4) LIBE);
5. carry out data protection impact assessment (Art. 33 (1) in conjunction with Art. 32a (3) LIBE);
6. hire a data protection officer (Art. 32a (3) (b) LIBE) – this obligation applies to the controller who will collect at least 5,000 data subjects. If the Beautician decides to use the services of a marketing company, she will formally become the controller of a database containing over 5,000 records.

AFTER TWO YEARS OF THE ACTIVITY, THE BEAUTICIAN SHALL:

1. review the applied policies (Art. 22 (1) LIBE); the review shall be documented (Art. 28 (1) LIBE);
2. carry out and document a compliance review (Art. 33a LIBE);
3. conclude specific entrustment agreements of the processing of personal data when allowing access to personal data to outside providers (for example, a company providing web hosting service). All the entrustment agreements shall be documented in writing (Art. 26 (3) LIBE) – an entrustment agreement concluded in the electronic version shall not meet the requirements.

THE ACQUISITION OF PERSONAL DATA

When the client of the Beautician gives any of their personal data, (e.g. before completing the questionnaire on health status), she will be obliged to publish on the website in the graphic and textual form the following information:

1. whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;
2. whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;
3. whether personal data are processed for purposes other than the purposes for which they were collected; Collecting data, e.g. for the purpose of the execution of the contract, the Beautician cannot exclude that if the client fails to settle the costs, the data shall not be used for the assertion of a claim. In this case, despite the fact that the assertion of a claim is a legitimate interest, the Beautician shall indicate that she does not comply with this obligation.
4. whether personal data are disseminated to commercial third parties; If data are made available to a web hosting provider or – in the case of claims – to a collection company, the Beautician shall indicate failure to comply with this obligation;
5. whether personal data are sold or rented out;
6. whether personal data are retained in encrypted form. (Art. 13a LIBE) – encryption does not seem necessary in this case. The Beautician shall disclose failure to respect this obligation, which could undermine confidence of the potential clients. The Beautician, though, will process personal data in accordance with the law.

THEN, THE BEAUTICIAN SHALL PRESENT TO THE CLIENTS AND DISPLAY THE FOLLOWING INFORMATION:

1. the identity and the contact details of the controller and data protection officer;
2. the purposes of the processing for which the personal data are intended;
3. the security of the processing of personal data, including the contract terms under which data will be processed, and the method of data processing, or how they meet requirements specified in Art. 6 (1) (f) LIBE;
4. the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
5. the right to request access to and rectification or erasure of the personal data and to object to the processing of such personal data, or to obtain data;
6. the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;
7. the recipients or categories of recipients of the personal data;
8. the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;
9. the logic involved in any automated processing;
10. any further information which is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected or processed, in particular the existence of certain processing activities for which a personal data impact assessment has indicated that there may be a high risk;
11. where appropriate, information whether personal data were submitted to public authorities during the last consecutive 12-month period.
    (Art. 14 LIBE)

Since the set of requirements is extensive, meeting the information obligation will entail reference to data processing policies. Drafting such a comprehensive and complex document requires knowledge of the rules and practice of data processing, which an average entrepreneur does not have.

In practice – still before the start of the business activity – the Beautician shall bear the costs of hiring a lawyer/data protection officer, who will develop privacy policies, consent clauses, a form implementing the information obligation, etc.

PROCESSING OF PERSONAL DATA FOR DOCUMENTATION PURPOSES

1. Having executed the contract, the Beautician may process her clients' personal data for purposes of proof (Art. 17 (4) (b) LIBE). The Beautician, however, may not keep the registry (e.g. in Excel format) of the clients' visits for such purposes as discounts for regular clients, remarks as to particular treatments (e.g. allergic reactions that have occurred). Completed orders shall not be subject to normal operations and shall be established in such a way that they cannot be changed anymore (Art. 17 (4) LIBE).
2. The Beautician shall be obliged to erase data after the completion of the processing, which in most cases will involve the purchase and implementation of appropriate software (Art. 17 (4) LIBE).

PENALTIES

Infringement of any of the above provisions of the Regulation shall involve the imposition of a financial penalty on the Beautician irrespective of the degree of responsibility (Art. 79 (2a) LIBE). Limitation of financial liability of the Beautician to intentional or negligent incompliance shall apply only in the case of possession of a valid European Data Protection Seal – Art. 79 (2b). In order to obtain such guarantee, the Beautican will need to incur additional costs of the audit – Art. 39 (2a). Due to the processing of sensitive data and any associated risks, the Beautician wishes to obtain such a seal. She should take into account this cost as the additional cost of conducting business activity.

COSTS

In order to meet the above obligations concerning implementation of the provisions of the Regulation, the Beautician shall bear significant costs of the preparation and maintenance of the required documentation, as well as organisational measures required by the Regulation.

The costs have been calculated with reference to the current market rates, need of the services provided by specialised consulting companies and serious legal and financial risk incriminating both the Beautician and the Beautician's service provider (e.g. the data protection officer), which always influences an increase in prices of services.

Given the need to use the services of a professional consulting company (implementation of the obligations requires specialist legal and often also technical knowledge, which the Beautician does not have), the amount of the expenditure in question can be estimated as follows:

1. drafting policies with regard to the processing of personal data and the protection of data subjects' rights (Art. 11 (1) LIBE) – PLN 6,000 net
2. preparation of informative clauses (Art. 13a and 14 LIBE) – PLN 600 net
3. implementation of compliance policies (Art. 22 (1a) LIBE) – a minimum of PLN 6,000 net
4. review and documentation of the risk analysis (Art. 32a (4) LIBE) – a minimum of PLN 6,000 net
5. arrying out data protection impact assessment (Art. 33 (1) in conjunction with Art. 32a (3) LIBE) – a minimum of PLN 6,000 net
6. preparation of written entrustment agreements on the processing of personal data for at least two entities (web hosting and software providers) – PLN 1,500 net.

The Beautician will need to conclude an agreement with a data protection officer (Art. 32a (3) (b) LIBE). The agreement shall be concluded for a specified period of time. The cost of such fixed service can be estimated (given the minimum amount of the processed data by the Beautician) at about PLN 1,500 net per month, that is **PLN 18,000 net per year**.

Every year, the Beautician shall bear the cost of the review and documentation of the risk analysis (Art. 32a (4) LIBE). This procedure shall be of the routine nature and its cost can be estimated at about PLN 1,500 net.

After two years of operation, the Beautician shall bear the costs necessary for the acquisition of the following services:

1. implementation and documentation of the review of applied policies (Art. 22 (1) LIBE); – PLN 1,500 net.
2. implementation and documentation of the compliance review (Art. 33a LIBE) – PLN 1,500 net.

It cannot be excluded that due to the processing of sensitive data, the cost of these services may be higher.

The total costs of the documentation requirements under the Regulation in the first two years of the Beautician's business activity can be estimated at not less than PLN 66 600 + VAT.

This sum covers only the costs of drafting and execution of documents and informative clauses, including the costs associated with legal services and services provided by the data protection officer.

The above estimate does not include the cost of activities necessary for the actual protection of personal data against loss and damage.

The estimate omits, in particular, the cost of purchasing the software for data protection, including anti-virus or cryptographic software, the acquisition costs of web hosting services on properly secured servers, backup costs, and finally, costs of physical security measures that should be introduced in the Beautician's seat.

Part 2.

The position of the Polish Confederation Lewiatan on the work progress on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM 2012/0011)

I. Introduction

In the era of the digital economy, accumulated, analyzed and adequately compiled data are a source of reliable and easily accessible knowledge about the phenomena, processes and trends that have been occurring. Its skillful use by the public authorities, entrepreneurs and citizens has been contributing to the socio-economic progress, and will be one of the main criteria deciding about the competitive position of Poland and the European Union in the world.

The entrepreneurs affiliated to the Polish Confederation Lewiatan are aware that the incompetent and reckless use of data, particularly personal data, may give rise to adverse effects and violate the rights and freedoms of citizens. It is the common interest to minimize such risks and eliminate any misuses. Europe needs a legal framework that will effectively safeguard the interests of citizens. At the same time, it must allow the use of data without generating unnecessary costs and obstacles in doing business and carrying out public tasks. According to the Polish Confederation Lewiatan, the current progress of works on the proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM (2012) 11 final) raises concern that the opportunity to create regulations corresponding to these challenges may be missed. After over two years of work on the Regulation, the European Parliament and the Council of the European Union presented their views on the shape of the EU legal framework concerning the protection of data[1]. The Polish Confederation Lewiatan supports the risk based approach of the Council. It is reflected in making information and documentation obligations imposed on the controller dependent on the nature of the data processing and the risks that may be associated with a possible violation of data security. We propose to move away from the requirement of an explicit consent to data processing and to release the controller from the obligation to notify data security violations to the supervisory authority and the data subject if they applied technical measures limiting the possibility of the use of data by unauthorized persons. We regard as positive limiting the definition of the recipient pursuant to the Polish law, as it is an important change in daily business operations.

The text of the Regulation proposed in the report of the European Parliament requires significant changes. Many of its provisions impose on the controllers disproportionate and costly obligations. Paradoxically, the adopted solutions will be often unfavorable also for the data subjects. The most problematic provisions include the legitimate interest of the controller, the general rules relating to the information and documentation obligations, the obligation to notify the data subject about violations and the unconditional right to object to data processing based on a legitimate interest of the controller.

Despite the above positive evaluation, some provisions have also been found in the text of the Council which we still consider to be problematic (prior consultation, data portability, the right to be forgotten). At the same time, we consider the approach of the Parliament better in relation to pseudonymized data (Article 10), prior consultation (with the supervisory authority or Data Protection Officer) and to the possibility of imposing an administrative fee in the case of excessive requests of data subjects.

Although we fully support the need to ensure the protection of the youngest Internet users, we support deleting the definition of a child from the Council's proposal. The introduction of effective mechanisms verifying age in the digital environment is problematic and should not (as noted in the report of the EP) lead to processing larger amounts of data.

Detailed comments on the texts of both institutions can be found below. We hope that in the course of further discussion in the Council and the Parliament, they will help to eliminate the provisions of the proposal that are unfavorable to entrepreneurs.

1 Adequately expressed in the European Parliament legislative resolution of March 12, 2014 and in the Report of the Irish Presidency of May 18 2013, summarizing the results of the Council's work on chapters I-IV of the project.

II Specific comments[2]

EXCESSIVE INFORMATION IS THE LACK OF INFORMATION

The Parliament's report has introduced a disproportionate set of information that the controller will be obliged to provide data subjects with before and during data collection (Article 12-15). Given the speed with which transactions are made, the consumer will not be able to read all the information, especially since the information on data protection is only a fraction of all the information that is provided to the consumer before concluding an agreement. What is more, data subjects will find much of the information, previously provided only to supervisory authorities, to be unclear. It will discourage consumers from reading the sent information and lead to even greater automaticity in granting consents. Neither will it increase public awareness as to the conditions of the data transfer and the way data are processed by the entities to whom they have been transferred.

According to the Polish Confederation Lewiatan, a more preferable text in this regard is the one of the Council since it introduces a limited scope of information, including obligatory information and other that should be provided if it is necessary to ensure fair and transparent data processing in a particular case. It is also important to allow the controller to inform about **categories of recipients (paragraph 1a, point c), and not the specific recipients to whom data will be transferred**. The controller is often unable to provide information about a specific recipient for the future and it is only possible to define categories of subjects to whom data will be made available.

A positive – from the point of view of entrepreneurs – solution introduced in the EP report (Article 12 (4)) is **the possibility to collect a reasonable fee by the controller** in the amount justified by the costs of handling data subjects' requests in case they are excessive. What raises some doubts, however, is the fact that paragraph 4 refers to the rights set forth in paragraph 1, from which the sentence about the articles has been deleted. While it is understandable that the request for access to data, the right to correct it and to object to data processing should be free of charge (subject to the above, if excessive), **it should not be forbidden to charge a fee for the implementation of the right to data portability**. We consequently emphasize that the right to data portability is a service and not a right of the data subject under the rules on data protection

INFORMATION ICONS (STANDARDIZED INFORMATION POLICIES)

The Parliament's position oblige the controller to inform the data subject about certain aspects related to the processing, before the collection of data. According to the Polish Confederation Lewiatan, providing such information in a graphic form should be **optional**. The use of icons will be impossible or ineffective to use in case of certain means of communication with the data subject. The system of icons can be useful on the Internet or in channels with limited space for transmission of information content (e.g. mobile applications). It may, however, be problematic in telephone contact with the data subject. Even now consumers seem to get annoyed when forced to listen to long pieces of information before getting through to a consultant.

Another problem is that the system of icons as proposed by the Parliament further extends the already comprehensive scope of information. **Any use of the system of icons should be a form of implementation of the information obligation** imposed on the controller in Article 14 of the EP position. We propose to harmonize Annex No. 1 and the content of Article 14, so that placing icons could be a(n) (alternative) form of complying with the information obligation, and not its extension. The system of icons currently proposed by the EP raises the following issues:

- The first two icons („No personal data are collected beyond the minimum necessary for each specific purpose of the processing" and „No personal data are retained beyond the minimum necessary for each specific purpose of the processing") require providing the data subject with the information that data are processed in accordance with Article 5 of the proposal of the Regulation. The value of this information to the data subject is small, since every controller is obliged to process data in

2 Adequately expressed in the European Parliament legislative resolution of March 12, 2014 and in the Report of the Irish Presidency of 18 May 2013, summarizing the results of the Council's work on chapters I-IV of the project.

accordance with these rules. In addition, the data subject will not be able to verify these declarations. Even if the controller, contrary to Article 5, collected more data than is necessary to achieve a given objective, it is difficult to imagine that they would openly admit to it.

- Icons 3-6 relate to the processing of data, which after meeting the conditions specified in the Regulation shall be seen as lawful. The system of icons does not make it possible to prove that the controller fulfills these conditions. As a result, such rudimentary information may give the data subject the wrong impression that the behavior of the controller which do not comply with the information contained in the system of icons – is unlawful. It could undermine the consumer's confidence in the legally operating companies and discourage them from using the companies' services.

For example, sharing data with some third parties, such as commercial entities of the same holding group based on one of the conditions of Article 6 is legal and often consistent with the interest of the data subject and the controller. However, it may be expected that the information about data transfer to third parties presented in the form proposed by the EP may give the data subject the opposite impression.

For these reasons, if the system of icons was introduced, **the entrepreneur should be able to present only the selected icons**, which due to the nature of the activities and foreseeable situations can be fulfilled by the controller. This would be a kind of declaration towards the data subject that the controller will not perform certain categories of processing.

ASSESSMENT OF THE EFFECTS OF PROCESSING, RISK ANALYSIS, REVIEW OF COMPLIANCE WITH THE RULES

The Parliament's report introduces a number of rules, which formalize the check of the compliance with the rules. It includes verification before the processing, assessment of the associated risks and activities to check the compliance. The relationship between the risk analysis (32a) and the assessment of the impact of processing (33) is not clear, and conducting both analyses would be a duplication of the same actions and documentation. **We propose to delete Articles 32a and 33a**.

LACK OF FLEXIBILITY AND COSTS

The provisions of the Parliament's text are too prescriptive. They do not leave the controller the possibility to adapt the processing standards (the amount of information provided to the data subject, processing procedures and their documentation, measures to ensure compliance, including the decision to hire the data protection officer) to the scale and nature of data processing. They impose a template – applicable to all data subjects – overlooking the technological content, scale and nature of data processing.

This is particularly evident in:

- the requirement to prepare extensive documentation (data processing policy, documentation of implementing the obligations arising from the provisions of the Regulation, documentation of the risk analysis and assessment of the processing effects),
- an extensive (and open) directory of information provided to the data subject,
- the requirement to appoint a data protection officer in the case of processing data of more than 5,000 people per year (this is not much in the case of data collection for a website, for example, for the purpose of newsletter mailings). This obligation also applies to any entity that buys (a legal) database containing data of more than 5,000 people in order to advertise its products and services (buying a smaller base is not a cost-effective practice),
- the scope of information to be notified in the event of a breach of security,
- the requirement to perform and update risk assessments and reviews of compliance of the processing,
- defining mandatory provisions of (the simplest) authorization agreement.

From all these responsibilities it follows that even the smallest data processing entities will be forced to use professional legal services to assure compliance with the regulation. Given the small number of people or entities having expertise in this area available in Poland, this may lead to a significant increase of the costs of data processing services– at least during the initial period of the application of the Regulation. In one way or another, this will increase the costs of starting and running a business, as well as hamper the functioning of companies.

LEGITIMATE INTEREST OF THE CONTROLLER

Granting the data subject an unconditional right to object in the situation when the processing is based on the legitimate interest of the controller (Article 19 (2) of the EP) will be dangerous for conducting everyday business. The provision does not provide for the possibility to assess whether the legitimate interest of the controller outweighs the interest of the data subject. Such an approach threatens the possibility to assert claims, prevent fraud, ensure safety in the workplace and protect other legitimate interests of the controller.

We assess critically also the limitation of the possibility to process data based on the legitimate interest of the controller only if it is consistent with the „reasonable expectations" of the data subject. The controller cannot predict what kind of processing is expected by the data subject. In addition, as noted above, even if the processing for a particular purpose goes beyond the data subject's expectations, it can be fully justified.

CONSENT

In relation to the consent, we emphasize the final sentence of Article 7, paragraph 4 (the EP), which forbids making the provisions of services contingent on the data subject's consent to process more data than is necessary to execute the contract. In our opinion, this prohibition will prevent data subjects from the access to free services, such as mailbox, social networking sites, press and music services, etc. The business model of these services is based on the financing coming from advertisers. In order to make the advertising space available on the websites of these services attractive, it is necessary to process some (pseudonymized) users' data. If the content provider is not able to finance their activities with the funds obtained (in exchange for users' data) from other businesses, such a business model will lose its viability. We emphasize that currently the vast majority of websites are financed by advertising. This is beneficial for citizens, the press, foundations and other entities conducting business on the Internet.

Leaving this provision in the final version of the text would also prevent the organization from organizing prize competitions and promotions, whose intermediate object is to obtain data of potential customers. We propose to delete this sentence. Promoting products and services makes an integral and legitimate part of any business, and such a provision would greatly restrict this possibility. It would also conflict with data subjects' rights to decide how they want to share their data and use the offered services.

In addition, we consistently emphasize that the requirement of the explicit consent in many situations may hinder the functioning of companies and may be unfavorable for data subjects. The way in which the consent is expressed should be relevant to the situation (context) in which it is expressed. For example, if the consumer requests a deferment of payment or release from debt, providing in justification their health data, such a request should be deemed as consent to process data necessary for this purpose. Similarly – after receiving a business card or e-mail address from another person – the entrepreneur should not ask for additional explicit consent. It should be reminded that it is the controller who has to prove that the consent has been obtained. Therefore, it will be in the controller's interest to ensure that the way of obtaining the consent is relevant to the conditions in which it has been expressed.

VIOLATION OF DATA SECURITY AND DEFINITION OF VIOLATION.

We support the version of the Council, both in relation to the definition of violation and to situations in which the supervisory authorities and data subjects shall be notified. In our opinion, however, it would be better to resign from setting a specific date of notification (as in the version of the EP), in favor of the obligation to submit such information without undue delay, which currently exists in Directive 2002/58 on privacy and electronic communications.

We also highlight the extension of the data violation definition in the version of the EP. It covers not only a breach of security but also all cases of non-compliance with the Regulation. The requirement to notify so broadly defined violations would be extremely troublesome and would flood the supervisory authorities with irrelevant – from the perspective of data security – notifications. We need to return to the definition of the European Commission and the Council.

PROFILING

We favor the approach adopted in the text of the Council. In our opinion, it protects the interests of data subjects allowing for the use of profiling for legitimate purposes of the controller, which does not significantly affect the data subject and has no legal effects. We emphasize the need to delete paragraph 1 (from the EP text) that allows an unconditional objection against profiling, regardless of whether the interest of the controller outweighs the interest of data subjects or not. This may undermine the possibility of profiling used to assess credit rating, prevent fraud and other legitimate purposes. In our opinion, the „objection" understood as the possibility to question the result of profiling should be granted to a decision based solely on profiling (as in the Council's text), and not against profiling as such, i.e. against the process itself.

- paragraph 2 (b) – we are in favor of the Council's text. We propose to delete the word "expressly" in Article 20, paragraph 2 (b) of the Parliament's text. We note that in fact the requirement to use profiling will not always be "expressly" specified in the legally binding acts , but this obligation often arises from the sector specific recommendations or those issued by the supervisory authorities. Regulations, for instance, in the banking, financial or insurance sector often impose on those entities a general obligation of responsible lending or prevention of fraud. Measures used for the implementation of this obligation, such as the use of rating or scoring methods based on the automated processing, are defined in the regulations issued by supervisory institutions, such as the Polish Financial Supervision Authority, or associations, chambers of commerce, etc. These acts often do not have the status of legally binding acts and rather represent the principles of good practice (e.g. in England, „Information Sharing Principles of Reciprocity") or act as recommendations. This effect would also be achieved by amending paragraph 2 (b) to read as follows: „Is expressly authorized by a Union or Member State law, in particular, codes of conduct or the requirements of supervisory authorities".

- paragraph 5 – we propose to replace the requirement to explain a decision based on profiling or human intervention by adding "shall provide suitable measures to safeguard data subject interests".

DATA PORTABILITY

We propose to delete this right from the proposal. According to the Polish Confederation Lewiatan, the institution regulated by this provision shall be understood as imposing on the controller the obligation to provide special services to the data subject, and not as an institution that protects personal data of the subject. The request for the transfer of personal data to another entity is not in any way related to the right to protect personal data. Imposing on the entrepreneur such obligation contradicts the freedom of establishment principle and the rules of the free market. Some concerns arise especially from the lack of interoperability of existing solutions. The need to ensure the possibility of data transfer between the systems may negatively affect innovation, as new solutions will have to interact with the existing ones. What also should be noted are the costs of adapting the currently used systems to this requirement. If however, the right to data transfer was to remain in the Regulation, it should take the form closer to the Parliament's version, and not the Council.

THE RIGHT TO BE FORGOTTEN

In our opinion, the Council's version better describes the situations in which the data subject will be able to exercise „the right to be forgotten" (paragraphs 1-3). **If this right of data subjects was to remain in the proposal of the Regulation, its implementation should be possible in well- defined cases**. It is important to clarify that data subjects enjoy this right only if the objection they submitted was effective (c). In paragraph 1 (d), it should be clarified that „the right to be forgotten" may be exercised only in the case of data processing without the legal basis from Article 6 (Lawfulness of processing), and not in the event of any inconsistency with the provisions of the Regulation. Therefore, we recommend to refer in point (d) to Article 6.

It should also be clearly indicated that the right to be forgotten shall not apply if the data have been collected and processed on the basis of statutory laws. This is particularly important in the case of data collection by the institutions established to assess credit rating or economic creditworthiness. The processing and access to such data is in the interest of all economic operators and is part of the actions undertaken by the European Commission. The efficient system of information on creditworthiness, and in particular the access to the same information, is crucial for the development and growth of the SME sector and for facilitating access of this sector to financing. If the right to be forgotten also applies to information providers and to data processed in order to assess credit rating (or even broader – creditworthiness), it may restrict the implementation of the objectives of these institutions, but above all, it may contradict the Commission's strategy for this sector[3].

For this reason, in the opinion of the Polish Confederation Lewiatan, paragraph 3 (f) – previously included in the Council's version – should be restored. The right to be forgotten shall not be granted if the data are needed for prevention, detection of fraud and other financial crimes, confirming identity and/or determining creditworthiness.

Despite the amendments made to the text, neither the version of the Parliament nor that of the Council answer the question how the controller – wanting to fulfill their obligation – could identify other controllers who process data that were made public. Even if in a given case it is possible, the controller cannot force any entities acting independently to perform such actions. This matter is better regulated in the Parliament's text, as it provides such obligation only in the situation when the data have been made public by the controller without a legal basis. However, the wording of Article 1 (c) needs to be changed in a way that enables the exercise of the right to be forgotten only if the controller's interest fails to outweigh the interest of the data subject, and not as it is now – unconditionally. We also propose to introduce such a restriction in Article 19 of the EP. We support (as above) – important from the controller's perspective – making the exercise of the right to be forgotten contingent on the possibility to verify the identity of the entity making the request (Article 17 (1a) of the EP).

Paragraphs 8a and 8b are to ensure the mechanisms monitoring the period of data processing and a periodic review of compliance of the processing with the rules. It should be noted that if they were to be implemented by adjusting data processing systems, unjustified costs will be generated. We propose to delete these paragraphs.

We consistently suggest removing a delegation for the European Commission from the Regulation (paragraph 9).

SENSITIVE DATA

We would like to note adding to the Parliament's version a category of "gender identity" to the directory of sensitive data. If this expression was understood as the sex of the data subject, such a change would be a big practical problem. The very letter addressing with a courtesy title (Dear Madam/Sir) or the use of the name that suggests the sex would be the processing of sensitive data and would entail some relevant restrictions. In order to avoid interpretation doubts, this kind of data should be deleted from the directory of Article 9. If it is not deleted, it is important to ensure that this expression will not be translated (and understood) as sex, but narrowly – as gender identity.

3 Brussels, 04/24/2013, SWD (2013) 156 final, Commission Staff Working Document; European Financial Stability and Integration Report 2012.

We propose to add to the point 1e of Article 9 that allows for the processing of sensitive „personal data which have been explicitly made public by the data subject" the following passage: „or voluntarily and at the request of the data subject transferred to the controller for a specific purpose specified by the data subject, where the processing is done in the interest of the data subject". This is important in situations when consumers provide their sensitive data at their own initiative, for example, when they request a deferment of payment or release from debt, providing in justification their difficult personal situation (e.g. illness). In order to execute the request (and therefore process these data), the controller should ask the data subject to send a separate consent to process sensitive data. It would be unfavorable and in practice troublesome both for the controller and the data subject. Since the consent to process data cannot be implied from the content of the data subject's request (explicit consent requirement), the extension of point 1e that we propose would enable to execute such a request without the need of obtaining a separate consent to process data for the purposes of the execution of the request.

PRIOR CONSULTATION

The provision requires to consult the supervisory authorities in a situation when the planned data processing may be associated with high risk.

In our opinion, the consultation should be optional. Even if data processing involves some risk, the controller may decide that he or she knows how to minimize it. The consultation requirement and waiting for the authority's advice shall impede the start of the business for 6 to 10 weeks (The Council's version). The Parliament's version is more favorable in the part which allows for "internal" consultations with the Data Protection Officer. This approach rightly reflects the principle of „risk based approach". The controller who is fully responsible for the processing of personal data should have the right to decide about the data processing, if according to their knowledge, they are capable of minimizing risks associated with a given processing. This is particularly justified in the case of controllers who use professional legal services or nominate a data protection officer.

RELATIONSHIP WITH THE SPECIFIC PROVISIONS AND INDUSTRY REGULATIONS

Despite the changes made to the proposals of the EP and the Council, there are still some doubts about the relationship between the provisions of the Regulation and the country-specific industry regulations or regulations of the supervisory authorities, such as financial supervisors. Implementation of some of the data subjects' rights would contradict industry provisions and would prevent economic operators and institutions from meeting the purposes for which they have been created. This is particularly important in the case of databases used by the banks to determine credit ratings, which helps to prevent fraud, as well as to determine creditworthiness of economic operators.

According to the Polish Confederation Lewiatan, the Regulation should decide that its provisions remain without prejudice to the specific provisions of the EU and member states regulating the processing of data in specific industries, which shall include also legal obligations arising from industry specific soft law regulations. This applies in particular to the recommendations of supervisory authorities, commonly used codes of good practice or collective agreements. The current wording of, say, Article 20, which allows for profiling only if it is **expressly** allowed by the EU or national legislation, may exclude this interpretation, for example, with regard to rating or scoring methods used by the banks or credit registers to determine credit risk and credit rating, which are applied pursuant not directly to the Act, but to the national and the EU supervisory bodies. In order to clarify it, we propose to introduce a general rule (Recital 36) that if data is processed to ensure a certain legal obligation is met, this obligation may result also from the recommendations of supervisory authorities.

POLISH CONFEDERATION
LEWIATAN

Polish Confederation Lewiatan is the most influential Polish business organisation representing employers' interests in Poland and in the European Union. Our aim is to support companies' development. We strive for stable economic growth, better legislation, healthy competition, more jobs and reinforced social capital. We associate 3 900 companies, which employ 900 000 workers.

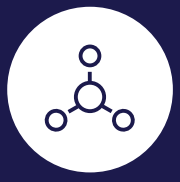
Our mission is to provide the best business conditions and support companies' competitiveness. For this reason, we are active in Poland, in the European Union and internationally. We are the only Polish employers' organisation with an office in Brussels since 2001. We also are a member of BUSINESSEUROPE, an organisation representing European employers' interests (41 business organisations from 35 countries, associating companies which employ 120 million workers). Our team of experienced experts and advisors cooperates with decision-makers on an ongoing basis. Lewiatan representatives sit on 450 councils, committees, groups and other decision-making bodies.

Lewiatan supports day-to-day activities and interests of its members and provides trade organizations with expert reviews. It facilitates business contacts and owing to the membership in international institutions, offers its members an access to international standards and know-how.

LEWIATAN

LEGISLATION
We try to ensure business friendly law and to protect companies' interests

KNOWLEDGE
We develop extensive economic expertise and provide current business information



NETWORKING
We make it possible for our members to establish relations with decision-makers and other companies

COMMUNICATION
We make the voice of business reach the public opinion

B2B
We support the development of member companies and their operational activities

Warsaw Office
Polish Confederation Lewiatan
ul. Zbyszka Cybulskiego 3
00-725 Warszawa, Polska
Tel. +48 22 55 99 900
Fax +48 22 55 99 910
lewiatan@konfederacjalewiatan.pl

Brussels Office
Polish Confederation Lewiatan
Brussels Office
Avenue de Cortenbergh 168
1000 Brussels, Belgium
Tel. +32 2 732 12 10

FREE COPY