RedFame

Business and Management Studies
Vol. 6, No. 1; March 2020
ISSN: 2374-5916 E-ISSN: 2374-5924
Published by Redfame Publishing
URL: http://bms.redfame.com

Analysis of the Impact of the GDPR on Third-Party Risk Management Programs and Related Recommendations for Domestic as Well as International Corporate World

Lucie Andreisová

Correspondence: Ing. Lucie Andreisová, Ph.D, University of Economics in Prague, Czech

Received: November 19, 2019 Accepted: December 17, 2019 Online Published: January 10, 2020

doi:10.11114/bms.v6i1.4683 URL: https://doi.org/10.11114/bms.v6i1.4683

Abstract

The General Data Protection Regulation (hereinafter also the "GDPR") has imposed several new rules on organisations (business companies) to protect EU individuals' personal data. Organisations that are data controllers or data processors need to have assurance that their third-party suppliers/vendors as well as sub-contractors comply with applicable GDPR requirements – in other words, they are now responsible for personal data managed by their third-parties. The question however remains, whether and how they are ready to manage this in their business practice? Compliance with the above indicated GDPR requirements comprises of a specific methodical approach that should be carefully integrated into the existing third-party risk management programs. The success of this integration builds on several crucial considerations. Before weighing those, it is important to understand how GDPR (Article 28 in particular) places new requirements on suppliers/vendors and affects the overall third-party relationships. Considering the above, this paper discusses the specific GDPR requirements which were enacted to strengthen companies' third-party risk management processes and includes a set of practical recommendations on how to establish/amend such programs in the corporate world.

Keywords: business company (corporation), compliance, IT and information security, statutory body, risk management, general data protection regulation (GDPR), supplier (vendor)

1. Introduction

1.1 The General Data Protection Regulation – A Brief Overview

The General Data Protection Regulation is a European law that acts as the primary regulation on how business companies protect European Union (hereinafter also the "EU") citizens' personal data. This law became effective on 25 May 2018 and extended the data rights of individuals, requiring organisations to take more steps to protect citizens' data with them or with their third-parties by taking the following steps (Garrubba, 2018):

- Developing dedicated privacy policies and procedures to protect personal data;
- Adopting appropriate technical and organisational safeguards to protect the individual's right to privacy.

Even though the regulation itself has undergone a vast amount of professional and/or public discussions, and has already been targeted by many academic writers, the author believes that the following key aspects of the GDPR should be reminded in the introduction of this chapter – as all of them do have a significant impact on the below introduced third-party risk management programs and related processes (Nulíček, Donát, Nonnemann & Lichnovský, 2017):

- Rights of individuals: The GDPR provides the individuals with enhanced rights regarding the processing of their personal data;
- Data protection officers (hereinafter also the "DPOs"): Business companies need to appoint a DPO (where large-scale personal data processing is required);
- Privacy by design: Business companies need to design dedicated internal compliance policies, procedures, processes and/or systems to ensure privacy of individuals' personal data straight in their very first/initial "design" phase (such internal processes are referred to as "privacy by design" and are being seen as core privacy safeguards[2]);
- Privacy impact assessments (hereinafter also the "PIA"): A PIA needs to be conducted for third-parties to identify and mitigate applicable data privacy risks;

- Data breach notifications: Data controllers must notify the data protection authority and data subjects of any personal data breach within 72 hours of detection.

But how does the GDPR influence cooperation with third-parties? Third-parties are essential to the way most business companies process and manage personal data[3]. The most recent research indicates that majority of data breaches include involvement of a third-party (NAVEX Global, 2018). In addition, the author believes that this figure is still to be growing – as hackers realise that technology platforms often represent an easily accessible entrepreneurial vulnerability (Ernst & Young Global, 2018). Under the GDPR, business companies now have a clear legal responsibility to select and manage their third-party data processors responsibly (Garrubba, 2018). The following text, among others, lays out the author's professional suggestions and/or practical recommendations for building and maintaining such an internal risk management framework (program) that would successfully mitigate the risks related to the use of third-parties (suppliers/vendors).

At its core, the GDPR positions numerous requirements regarding how business companies, regardless of their industry or location, manage the personal information of European "data subjects" (*i.e.* customers and employees). This regulation replaces the EU's Data Protective Directive (Data Protection Directive 95/46/EC), which had been the basis for EU laws that governs data privacy. It is important to realise that – in general – an EU regulation is legally binding in each member state, whereas EU directives identify results each member state is required to achieve through national laws (which can be developed by each state on its own) (Schenkov á & Las ák, 2017). Many of the ways that GDPR differs from the previous directive require third-party (vendor) risk management capabilities to be significantly updated and enhanced. Those changes should include (Vaswani, 2018):

- The extension of legal obligations to service providers (which the regulation refers to as "data processors" – see below);
- A broader definition or so called "higher classification" of personal data (sensitive data) that must be protected;
- New operational requirements for data processing (see below);
- Severe consequences for violations, including a maximum fine amounting to the greater of €20 million or 4 percent of global revenue[4]; and
- A new set of requirements for third-party data processors, as laid out in Article 28 of the General Data Protection Regulation.

The GDPR also introduces a brand-new terminology. Four of the most relevant phrases (with regards to third-party risk management processes) include:

- (Data) processing, *i.e.* any operation or a set of operations – either automated or manual – performed on personal data, including collection, recording, organization, storage, adaption, alteration, retrieval, consultation, use, disclosure *etc.*;
- Data subject, *i.e.* a person whose personal data is to be collected, stored or processed;
- Data controller, *i.e.* the entity or organisation (a business company/business corporation) that determines the purposes ("why"), conditions and means of processing of personal data ("how");
- Data processor, *i.e.* an entity (a supplier/vendor) that processes personal data on behalf of the controller.

In addition to the above, it shall be noted that Article 28 of the GDPR requires a closer analysis for business companies and vendors that qualify themselves as "processors" and must thereby comply with the new rules. In other words, Article 28 identifies the technical and procedural measures that the data processors are required to implement. This section also stipulates that data controllers (*i.e.* business companies that use vendors/suppliers which are being qualified as data processors) should only use those processors, which provide "sufficient guarantees" on being fully compliant with the individual requirements of the regulation[5]. These requirements, which are incorporated into 10 brief sub-sections, specify contractual requirements, rules related to processor's use of other processors, required codes of conduct, various certification mechanisms *etc.* (all applicable details are available below).

Achieving the desired level of compliance with the GDPR thereby requires a comprehensive, multi-step process that works in conjunction with an organisation's existing third-party risk management program. In summary, domestic as well as international undertakings should identify their critical vendor relationships and, after having clarity on that, they should further (Galdies, 2019):

- Understand which GDPR requirements clearly apply to the concerned vendor/supplier (third-party);
- Assess the third-party's level of GDPR (data privacy) compliance;
- Assess the third-party's overall security posture;

- Track how the third-party retains, accesses and transfers sensitive data;
- Amend and update respective contract provisions to ensure that they reflect all applicable GDPR requirements;
- Define key compliance items for satisfactory due diligence responses; and
- Conduct testing of key privacy and IT/information security-related controls.

A detailed "manual" on how to implement and/or adapt the already existing (internal) third-party risk management programs so as they meet the applicable GDPR requirements is being introduced in the text below.

2. How to Manage Third-Party Risk Under the GDPR[6]

2.1 General Comments and Recommendations

The following process should be treated as a basic risk management framework focusing on third-parties and their GDPR (data privacy) compliance. Whilst the sequence and emphasis of different phases may vary within each undertaking, all steps as proposed below should be existing and demonstrable. Demonstrability and accountability are fundamental requirements of GDPR (data privacy) compliance (Bowdler & Kettle, 2017). There should also be clear roles and responsibilities allocated within each business company – to ensure that these steps are utilised as legally or otherwise required. Those roles and/or responsibilities should be clearly documented (Andreisová, 2017).

As indicated above, any process like this must not only be implemented, but also further maintained, *i.e.* seen as an ongoing one. One-off third-party risk management programs reduce the risks only in a short run (*i.e.* from the short-term perspective) (Drastich, 2011).

Also, one of the most frustrating but at the same time the most valuable aspects of third-party risk management programs involves reconciliation of relevant business processes (*i.e.* how are they executed in business practice) to internal procedures (*i.e.* documentation that identifies how the applicable processes should be performed). The very first question should therefore relate to "How things work in practice?" The goal is to find out how processes are being performed before looking at how that same processes are being documented in the formal (internal) procedures. Based on author's professional experience, it is very often the case that severe discrepancies are being found when conducting such reconciliations. This can happen for several reasons – *e.g.* procedures are not being adequately updated to reflect the applicable technology changes. Such gaps must be identified and properly remediated (or potentially fully eliminated). After all, internal procedures often represent the record that various enforcement teams use to hold the organisations accountable (please see the two enforcement cases mentioned above).

It is a matter of fact that most multinationals already operate an internal third-party risk management program to address their suppliers'/vendors' IT and information security (data privacy) risks (NAVEX Global, 2018). These programs often include maintaining an inventory of third-parties, as well as the type of data they process; requiring vendors to adopt standard contractual clauses addressing IT and information security; and vetting vendor responses to security due diligence questionnaires (Andreisová, 2017). A growing number of business companies also include potential on-site IT and information security reviews and/or audits in their internal programs (NAVEX Global, 2018).

To address and comply with the applicable GDPR third-parties related requirements, companies doing business in Europe should consider creating an action plan that enhances their existing third-party risk management programs with the following components (PwC Global, 2018):

- Adding new GDPR-related criteria to their vendor risk-ranking formulas;
- Adding data privacy-related requirements to the standard contractual clauses and rolling those addendums out to impacted third-parties;
- Adding data privacy-related requirements to due diligence questionnaires;
- Adding additional data privacy-related controls to onsite audits (reviews); and
- Enhancing the frequency of ongoing monitoring to detect changes in the scope of suppliers'/vendors' data processing and facilitate reporting of data privacy impact assessments and suspected compromises of EU personal data.

Although business companies themselves have the ultimate decision on when due diligence assessments and processes should be performed, it is important to evaluate all third-parties that may impact the rights and freedoms of natural persons. Unfortunately, an exhaustive list of processes or activities that would require such assessment does not exist – and the author believes that it is impossible to create a generally applicable one (as this can certainly differ undertaking to undertaking). Regardless of the above, it shall be noted that the GDPR has provided some basic guidance and sample scenarios for further professional (corporate) consideration. As an example, the guidance includes the following (Vaswani, 2018):

- A third-party is, or will be, performing a high-risk process or service which may impact the rights and freedoms of natural persons;
- A third-party is, or will be, systematically monitoring a large scale publicly accessible area;
- As referred to in Article 9(1) of the GDPR, any third-party processing special categories of data on a large scale and/or personal data containing criminal convictions or offense;
- A third-party is, or will be, evaluating personal aspects relating to natural persons based on automatic processing, including profiling, and on which decisions are based that produce legal effects concerning the natural persons;
- A third-party is, or will be, leveraging new technologies, or those of a type in which no data protection impact assessment has yet been carried out;
- A third-party is, or will be, performing additional processing activities which require the completion of a data privacy impact assessment as defined by the supervisory authority.

Additional processing activities and businesses to consider may be the following ones (Garrubba, 2018):

- Customer facing activities;
- Activities related to children;
- Marketing and advertising activities;
- Digital transformation activities;
- Geolocation data;
- Profiling data;
- Public services;
- Mass communications;
- Joint ventures; and
- Global business operations.

2.2 A Five-Step Process to Achieving GDPR (Data Privacy) Compliance

2.2.1 Data Mapping and Discovery

The GDPR mandates that larger organisations are required to maintain dedicated documentation including comprehensive details of all processors[7]. However, the recent research shows that in today's corporate practice it is often the case that many business companies are not sufficiently aware of the full range of third-parties that are engaged in their business activities (NAVEX Global, 2018). As an example, cloud-based services can often be engaged outside of standard procurement processes and thereby also beyond the traditional IT and information security controls. It shall be highlighted though, that it is impossible to manage third-party risks without a complete understanding of who they are and what they do (Galdies, 2019). The first recommended step is therefore to develop a robust internal process to build and maintain a full list of potentially high-risk vendors/suppliers which needs to identify and describe for each processor the following areas (Galdies, 2019):

- Who – What data processor, who are the main contacts for data privacy, who are its sub-processors *etc.*
- What – Which data types are being processed?
- Why – What purposes are being fulfilled?
- Where – Where does the data processing take place, including sub-processors?
- When – How does retention work, when is data deleted/anonymised *etc.*?

Apart from the above, the question for the corporate world remains the following: "Which suppliers (vendors) and third-parties in general shall be seen as potentially high-risk, *i.e.* how to compile the list of potentially high-risk suppliers (for further risk-investigation)?" The author believes that a set of following key initial assessment questions may serve as a good practical example/instrument (please note that this is the author's own recommended list):

- Does the supplier have (or will it be given) access to company's internal systems/applications/network?
- Is the supplier critical to the concerned company (*i.e.* is there a high level of dependency of the concerned company on products/services delivered by this supplier/vendor)?
- Is the supplier being sent (or will it be sent) company's data (hard or soft copy), or collects data from other

sources on behalf of the company? Please note that this can be part of the following (and a proper definition/internal understanding of those categories should always be given out): customer data, colleague data, customer finance or payment data, commercially sensitive data, sensitive personal data, customer or colleague analytical data *etc.*

- Has the supplier/vendor been involved in any incidents or data breaches?

Building and maintaining the supplier list as described above (*i.e.* the internal list of potentially high-risk suppliers/vendors) is often best achieved by using an appropriate mixture of questionnaires, interviews and reconciliations with other sources. Based on author's professional experience, it can be recommended to consult the above with various internal stakeholders – such as supply chain (procurement) representatives and/or individual buying or business managers. After that, a dedicated "triage" questionnaire can be sent to each supplier to either confirm or refute the estimated risk-rating. Such triage may include – for example – the following (please note that these are the author's own professional recommendations):

- Detailed description of goods/services provided by the supplier (vendor) – *i.e.* what and where is being supplied (which jurisdiction and potentially also for which internal departments and business units);
- Cost/value of the contract;
- Which types of data are being held, collected, processed or transmitted by the supplier/vendor (and in which volume) – please note that a detailed description is required here;
- Confirmation on whether the supplier/vendor is critical to the concerned company;
- Confirmation on where the data is being/will be stored (*i.e.* whether is stays with the concerned company or with the supplier, in a data-centre managed by a third/professional party *etc.*);
- Confirmation on whether the supplier/vendor has been dealing with a security incident in the past;
- Confirmation on how the data at rest/in transit is/will be secured;
- Confirmation on who specifically has access to the data (*e.g.* employees of the supplier/vendor, its contractors *etc.*); and
- Confirmation on which contracts (and specific annexes) were signed (are to be signed in the future).

Based on "triage results" above, the supplier/vendor (third-party) should be assessed as high, medium or low-risk (*i.e.* the initial estimation of risk-rating either confirmed or refuted). For any high or medium-risk suppliers, a further risk assessment stage with the use of "detailed questionnaires" and potentially also "on-site reviews/audits" is recommended (see the subchapters below).

2.2.2 Policies and Contractual Documentation

As mentioned above (Article 28 and 35), organisations now have a legal obligation to establish contractual agreements between controllers and processors which clearly define the roles, responsibilities and liabilities of both parties[8]. The goal of each contract is to include (at a minimum) (PwC Global, 2018):

- The subject-matter and duration of processing;
- The nature and purpose of processing;
- The type of personal data and categories of data subjects;
- The minimum terms or clauses required of the processor; and
- The obligations and rights of the controller.

These articles ensure that organisations not only comply with the applicable GDPR requirements, but they also ensure that controllers and processors provide appropriate protection over data subjects and their personal data.

All business companies which are in scope of the above described regulatory principles should therefore have adequate policies and processes for ensuring data privacy (GDPR) compliance in place. Those should be enacted with the use of standardised data processing agreements (hereinafter also the "DPAs"), non-disclosure agreements (hereinafter also the "NDAs") and additional supplier contracts – such as, for example a supplier data obligation document summarising the individual IT and information security-related requirements/controls of a concerned company (*e.g.* information security and data governance controls; personnel security controls; controls for managing sub-contractors; controls for managing data subjects' and other requests; provisions related to controlling access to internal data; controls related to transferring internal data; controls related to incident management; controls related to back-up and disaster recovery; controls related to system development; controls related to physical and environmental security; controls related to

demonstration of compliance *etc.*). Such framework must be maintained over time – as all agreements with third-parties must reflect the acceptable minimum data processing terms (*i.e.* both existing as well as new agreements).

This documentation serves as an important tool in managing relationships with third-parties; and, in addition, it also provides for a great evidence of company's privacy commitment and lays down the groundwork for negotiation and selection of only those suppliers, who can operate to the standards expected by the concerned entity.

Least but not last, some other points to remember when contracting may include (ISO/IEC 27001:2014, Information Security Management Systems):

- The scope of third-parties data processing being undertaken;
- Information on how breach reporting is expected to work in practice;
- Information on how the third-party should handle data subject rights requests;
- Clear contact points and suitable review periods; and
- Realistic warranties and indemnities.

2.2.3 Detailed Risk Assessment

If the triage phase confirmed a higher risk-rating, the detailed risk assessment phase should be initiated as soon as reasonably possible. This phase should include all relevant (internal) stakeholders and should enable collection of all applicable details around the supplier risk.

Based on author's professional experience, it is now becoming quite common for business companies to issue standardised questionnaires to high or medium-risk suppliers to understand their capabilities and also the way of managing privacy and security-related measures. Such dialogue is a very valuable step in assessing and evaluating the supplier risk – however, it is important to ensure that the right questions are being asked. Below is a short summary of author's personal (professional) recommendations, *i.e.* the following areas should be discussed, understood and assessed:

- Security governance – *i.e.* a set of questions/controls around governance-related measures in the supplier's internal IT and information security program – *e.g.* who is accountable for IT and information security, how is statutory reporting ensured, is there an internal information security policy or equivalent in place, are there any sub-contractors in use, does the supplier have any internal certification or other standard (*e.g.* ISO 27001) *etc.*;
- Privacy – *i.e.* a set of questions/controls around breach reporting, management of data subjects' requests, privacy impact assessments, management of records of processing *etc.*;
- Risk management – *i.e.* a set of questions/controls around risk management-related measures applicable to the supplier/vendor – *e.g.* has the supplier published or adopted an information security risk management methodology, has it been approved by the statutory management, what is the information security risk management process for new projects before they go live *etc.*;
- Physical security – *i.e.* a set of questions/controls around physical environment of the supplier/vendor – *e.g.* its offices, data-centres, computer rooms *etc.*, including how the physical access is controlled and monitored;
- Personnel security – *i.e.* a set of questions/controls around employee screening and background checks, conflicts of interest *etc.* (this should relate to supplier's employee/contractor base);
- Host-based (endpoint) security – *i.e.* a set of questions/controls around securing supplier's endpoints and servers – *e.g.* firewall solutions, anti-virus, intrusion detection/protection systems, patching and vulnerability scanning *etc.*;
- Network security – *i.e.* a set of questions/controls around securing supplier's network – *e.g.* data separation, remote access and multifactor authentication, secure configuration standards *etc.*;
- Access control – *i.e.* a set of questions/controls around supplier's approach to passwords with regards to complexity, length, account expiry, lock-out period, available attempts *etc.*, including service and administrator accounts;
- Data security – *i.e.* a set of questions/controls around supplier's data classification and data handling processes, data retention and data destruction policies *etc.*;
- Logging and monitoring – *i.e.* a set of questions/controls around logging and monitoring of security and other events across supplier's IT environment; and
- Business continuity – *i.e.* a set of questions/controls around business continuity and disaster recover processes

(and plans).

Least but not last, like all good interviews the questions raised should always focus on "open" rather than "closed" questions, *i.e.* the preferred approach is to ask "how" rather than "do you". The received results should then be carefully considered, the risk of the individual responses assessed in the overall context of supplier's organisation and sorted out into three main groups: compliant, partially compliant (acceptable risk with no remediation needed), not compliant (unacceptable risk with dedicated remediation needed). Where risks are assessed as unacceptable, the individual gaps must be identified, and a dedicated remediation (action) plan agreed with the supplier prior to placing the work. If the above is not possible, a different supplier should be selected.

Other recommendations would include using the updated documentation and regular (at least annual) re-assessment of the risk-level and specific risks of each cooperation – as the new regulation also states that DPOs or appointed privacy leaders who are aligned to a controller or a third-party processor are expected to monitor company's compliance with GDPR on an ongoing basis – therefore, ongoing monitoring activities, processes and measures should be evaluated and updated as part of "business as usual" activities and operations. In addition, third-party relationships may evolve over time, so business companies need to be flexible and adapt their strategies to effectively manage changes in the level and types of risks associated with each relationship (external cooperation).

2.2.4 Auditing

Where the supplier risks appear to be "high", the processing itself is seen as sensitive, the results of the detailed risk assessments appear to be unclear or – based on assessor's professional knowledge and intuition – "too good to be truth", or where there has been a security or other incident with the supplier in the past, an on-site audit or review can be recommended (remember that all the above phases are self-assessments only – conducted by the supplier/vendor internally).

A reliable audit will be both interview and evidence-based and will include (Drastich, 2011):

- How does the processor (supplier/third-party) meet the applicable GDPR requirements in its business practice?
- How does the processor (supplier/third-party) manage data subjects' requests in its business practice?
- How do the data breach identification and reporting processes work in supplier's business practice?
- How can evidence on internal policies and training and comms activities be demonstrated?
- How are other security measures and processes in place understood by the supplier and its employees, contractors *etc.*?

Importantly, all assessment results should always be shared with respective internal stakeholders (such as procurement and business managers – see above). A good practice would be to go through all the controls from the detailed risk assessment phase when being on site with the supplier and review all related documentation and other evidence in person (Hertzberg, 2018).

2.2.5 Remediation and Continuous Monitoring

Both the detailed risk assessment and third-party audit stages can result into identification of various gaps/issues and thereby also further risks. Sometimes those risks will be acceptable, but in many cases, something will need to change to ensure the data processing is seen as fully compliant.

Before the third-party is approached with specific proposals for remedial actions and plans, the remediation must be agreed internally with all key stakeholders (see above). Any remedial action plan or action itself must be carefully explained and accepted by the concerned third-party (and above all documented). Any potential progress should be continuously monitored and once completed, the related control(s) thoroughly tested and a formal sign-off received (Schenkov á & Las ák, 2017).

To sum up, third-party processors may constitute significant business and other risks, however, implementing the above proposed five-step third-party risk management program should mitigate those risks appropriately.

3. Conclusion and Discussion

As described an evidenced in the main part of the paper, the European Union's General Data Protection Regulation has significantly increased the risk of outsourcing data processing activities of business operations involving European individuals to third-parties – as the regulation expands the scope and complexity of third-party risks for (not only) large multinationals, which often engage thousands of suppliers/vendors that perform some type of processing of EU personal data. These business companies need an action plan and ongoing risk management capability to mitigate the potential GDPR enforcement, litigation and other risks related to their supply chain.

As presented above, primarily the following five articles of the GDPR are adding new requirements or somehow deepening the existing obligations from the legacy 1995 EU Directive on Data Protection (Axinte, Petrica & Bacivarov, 2018):

- Article 28 (Processor) requires contractual protections with data processors and their sub-processors, adequate data protection, and production of evidence of compliance with the GDPR;
- Article 30 (Records of processing activities) requires data processors to maintain a detailed inventory of the EU personal data they host;
- Article 32 (Security of processing) requires data processors and their sub-processors to implement comprehensive IT and information security-related controls to protect EU personal data;
- Article 33 (Notification of a personal data breach to the supervisory authority) requires data processors to report compromises of EU personal data to their clients without undue delay; and
- Article 36 (Prior consultation) requires data processors to provide data protection impact assessments to their clients in certain high-risk situations.

In addition, the GDPR is not a one-off implementation regulation, but an ongoing one that – among others – requires periodic risk assessment of third-party suppliers/vendors. Business companies are therefore required to align their existing third-party risk management frameworks with the applicable GDPR requirements. The following summary represents a brief view on the key components of a "GDPR-compliant" third-party risk management framework (Vaswani, 2018):

- Gap analysis: Organisations need to perform a gap analysis to assess the current state of data protection rules and identify how data is flowing and used by third-parties and their sub-contractors.
- Differentiating between data controllers and data processors: Organisations need to classify third-parties as either data processors or data controllers.
- Contract review: Organisations now have a legal obligation to establish contractual agreements between data controllers and data processors, with the terms clearly defining roles, responsibilities and liabilities of both parties.
- Conducting data privacy impact assessment: Organisations now need to conduct a privacy impact assessment to identify and mitigate the data privacy risk(s) of third-parties and to assess third-party readiness in complying with the GDPR.
- Continuous monitoring: Organisations need to continuously monitor the third-parties and their sub-contractors to identify data privacy risk(s) and set alerts for high-risk third-parties and their sub-contractors.
- Mechanism(s) for incident reporting: Organisations need to enable incident reporting mechanisms for internal departments and their third-parties to report data privacy incidents and their potential impact. The regulation requires data breach notifications to be available for supervisory authorities within 72 hours of detection.
- Ensuring third-parties are compliant: Organisations need to make sure that their third-parties are GDPR-compliant and follow strict policies and controls that are aligned with their own policies and controls.

When implementing/amending the components listed above, the following key considerations shall be taken into account (Vaswani, 2018):

- Know your data: Business companies should know how third-parties access, store, process, use and transfer the personal data.
- Extensive screening for third-parties onboarding: Business companies should expand the scope of due diligence of third-parties by adding privacy-related requirements and conducting a data privacy impact assessment while onboarding new third-parties (suppliers/vendors).
- Third-party contracts: Business companies should review legal clauses in contracts with third-parties to ensure that they meet respective GDPR-related requirements.
- Improvement of third-party risk assessments: Business companies should identify and communicate with data owners, perform IT and information security risk assessments for all third-parties that have access to "their" personal data and enhance the risk management frameworks with GDPR requirements.
- Risk-based continuous monitoring: Business companies should continuously monitor the high-risk third-parties.
- Update of the third-party risk management processes: Business companies should profile their third-parties,

classify them based on criticality and appoint a Data Privacy Officer (DPO) for monitoring the level of GDPR (data privacy) compliance of third-parties in scope.

- Implementation and monitoring of data privacy controls: Business companies should define controls to protect personal data and continuously monitor the effectiveness of those controls. Also, companies should make sure that they define controls for data processing, accessibility, audit, record maintenance, subcontracting *etc.*
- Establishment of data privacy-related policies and procedures: Business companies should establish policies and procedures to detect data breaches and establish incident reporting mechanism(s) for internal as well as external use.
- Enhancement of IT/information security systems: Business companies should enhance respective IT and information security systems to comply with applicable GDPR requirements.
- Audits: Business companies should add IT and information security-related controls to the existing audit plans.

The above can be achieved by using the practical five-step risk management framework proposed by the author in the main body of this paper. That process consists of:

- Data mapping and discovery;
- Policies and contractual documentation;
- Detailed risk assessment;
- Auditing; and
- Remediation and continuous monitoring.

Least but not last, it shall be once again highlighted that achieving the required level of GDPR (data privacy) compliance is not the same as sustaining that compliance. The same external disruptions and internal changes that created gaps between the applicable business processes and written procedures are occurring within data processors and other critical suppliers/vendors. That is the reason why the most effective GDPR programs, as well as the best third-party risk management frameworks, contain at least some form of ongoing monitoring activities (Andreisová, 2017).

Acknowledgements

This paper has been supported by the Internal Grant Agency ("IGA") of the University of Economics in Prague, project ref. IG207019.

References

Andreisová, L. (2017). Current Trends in the Global Compliance Environment. Business Law in Selected EU Member States – Proceedings of IX. *International Scientific Conference. Prague: TROAS,* 304 p. ISBN: 978-80-88055-03-7.

Andreisová, L. (2017). Duty of Care of Members of Statutory Bodies in Capital Business Companies and its Relation to Internal Compliance Programs (dissertation). *Prague: University of Economics, Faculty of International Relations.*

Axinte, S. D., Petrica, G., & Bacivarov, I. (2018). GDPR Impact on Company Management and Processed Data. *Quality-Access to Success, 19*(165).

Bowdler, J., Kettle, R., & coll. (2017). Diploma in Governance, Risk and Compliance: Course Manual. *Birmingham: International Compliance Training Ltd*.

Drastich, M. (2011). Information Security Management Systems. *Prague: Grada Publishing,* 128 p. ISBN: 978-80-247-7616-3.

Ernst, & Young Global Limited. (2018). Cyber threats are a priority for managers in risk management. Lack of experts leads to outsource selected activities. *Prague: EY Global,* 2018. Retrieved from https://www.ey.com/cz/cs/newsroom/news-releases/2018_kyberneticke-hrozby-jsou-pro-manazery-prioritou-v-rize ni-rizik

Galdies, P. (2019). Steps for Managing the GDPR Third-Party Threat. *London: DQM GRC,* 2019. Retrieved from https://www.dqmgrc.com/article/6-steps-managing-gdpr-third-party-threat

Garrubba, T. (2018). Expect the Unexpected: 5 Keys to Managing Third-party GDPR Risk. *Santa Fe: Shared Assessments.* Retrieved from https://sharedassessments.org/expect-the-unexpected-5-keys-to-managing-third-party-gdpr-risk/

Hertzberg, J. (2018). GDPR AND INTERNAL AUDIT: Auditors can help their organization navigate the compliance

risks posed by Europe's General Data Protection Regulation. *Internal Auditor, 75*(4), 22-24.

ISO/IEC 27001:2014. *Information Security Management Systems.*

NAVEX Global, Inc. 2018 Ethics & Compliance Third-party Risk Management Benchmark Report. *Navex Global: London*. Retrieved from https://www.navexglobal.com/en-us/resources/benchmarking-reports/2018-ethics-compliance-third-party-risk-management-benchmark-report?RCAssetNumber=4022

Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., & Tomíšek, J. (2017). GDPR. General Data Protection Regulation (practical commentary). *Prague: Wolters Kluwer,* 544 p. ISBN: 978-7552-765-3.

PwC Global Limited. (2018). An action plan for tackling third-party GDPR risk. *PwC Global: United States of America*. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/general-data-protection-regulation/third-party-risk-management-gdpr.html

Regulation (EU). 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A32016R0679

Schenková, K., Lasák, J., & col. (2017). Compliance in Business Practice. *Prague: C. H. Beck,* 480 p. ISBN: 978-80-7400-668-5.

Vaswani, V. (2018). Rethinking Third-Party Risk Management (TPRM) in the GDPR Regime. *London: Corporate Compliance Insights*. Retrieved from https://www.corporatecomplianceinsights.com/rethinking-third-party-risk-management-tprm-in-the-gdpr-regime/

Notes

Note 1. Dr Lucie Andreisová is a graduate from 'Business and Law' master's degree program at the Faculty of International Relations, University of Economics in Prague. In 2017, she has successfully accomplished there her Ph.D. in 'International Business Law' (with a closer focus on business ethics and corporate governance). At this department, she is actively lecturing since 2012. Lucie has devoted herself to the topics above and continues to pursue them in her professional career – as she was, for over five years, responsible for Governance, Risk and Compliance ("GRC") in Vodafone Czech. In 2015, she was also employed as Senior Compliance Specialist in Société Générale, where she got a more detailed knowledge of regulatory compliance. Between y. 2017-2018, Lucie was holding a position of Compliance Manager in Vodafone Group, London. Currently, she is holding a role of CE Head of Compliance & Ethics at Tesco Stores Czech, where she was previously employed as CE Lead IT and Information Security Manager. Since 2017, Lucie also acts as an Assistant Professor at the Department of Business and European Law and is a member of the Czech and International Compliance associations, where she's accomplished the ICA Advanced Diploma in GRC (y. 2018). A summary of her publications is available online (insis.vse.cz).

Note 2. For more details please see, for example, the following paper: Kurtz C., Semmann M., Böhmann T. Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors. Presented at the Americas Conference on Information Systems (AMCIS), New Orleans: 2018.

Note 3. Including everything from cloud platforms for data hosting, cloud hosted finance and HR applications to marketing agencies and, for example, also web technologies.

Note 4. The latest GDPR-related enforcement cases include British Airways (for further details please see – for example – the following article: "British Airways faces record £183m fine for data breach" at https://www.bbc.com/news/business-48905907), and Marriott (for further details please see – for example – the following article: "UK proposes another huge data fine. This time, Marriott is the target." at https://edition.cnn.com/2019/07/09/tech/marriott-data-breach-fine/index.html).

Note 5. "When entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation."

Note 6. Please note that apart from the below mentioned citations and references, this part of the text represents author's personal proposals and recommendations (derived from her own professional experience and subject matter expertise).

Note 7: GDPR Article 30: "Each controller and, where applicable, the controller's representative, shall maintain a

record of processing activities under its responsibility."

Note 8: GDPR Article 28: "A processor shall be governed by a contract … … that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller." and GDPR Article 35: "Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."