The Interplay Between the GDPR and the IDD

Viktoria Chatzara

1 Introduction

The operation of the European Union insurance industry during the last years has been deeply disrupted by the adoption in 2016 and the entry into force in 2018 of the General Data Protection Regulation (the “GDPR”)¹ and the Insurance Distribution Directive (the “IDD”),² which have caused significant changes to the EU and national markets. In some cases these changes have even affected non-EU market players, as in the case of the GDPR provisions, the scope of which also covers companies established outside the EU, but offering products or services to EU-located individuals or monitoring the behavior of individuals within the EU.³ In other cases the implementation of the new rules has resulted in radical transformations of the insurance market.⁴

¹Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

²Directive (EU) No. 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast).

³See in this relevance Article 3(2) of the GDPR, as well as Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)—Version adopted after public consultation by the European Data Protection Board (EDPB) on 12 November 2019, and available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf.

⁴As, for example, in the case of the Greek Law 4583/2018 transposing the IDD, Article 5 par. 7 of which prohibited the cooperation between insurance agents and insurance brokers, thus obliging

V. Chatzara (✉)
Rokas Law Firm, Athens, Greece
e-mail: v.chatzara@rokas.com

1.1 *Similar Origins and Parallel Lives*

Both the GDPR and the IDD have parallel “life stories”, as they both come to respectively replace previously applicable EU laws on data protection (namely the Directive 95/46/EC) and on insurance mediation (namely the Directive 2002/92/EC), aiming to address any issues that rose from the implementation of the previous laws, and also to modernize the applicable legal framework in the data protection and insurance distribution field.

As a coincidence that added to the regulatory compliance burden of the insurance industry participants that were affected by these new sets of rules, both the GDPR and the IDD were enacted in 2016 (May and January respectively), and became effective in 2018 (May and October⁵). With respect to the GDPR, although it granted the national legislators the possibility to adopt more detailed and/or stricter provisions in relation to certain issues,⁶ for which it is often mentioned as “hybrid” Regulation, its provisions became directly applicable and enforceable, as provisions of an EU Regulation. On the contrary, in order for IDD to become applicable, the national law measures transposing it into the legal orders of each Member State needed to be enacted.

Root Causes and Aims Both the GDPR and the IDD were adopted by the European Union in the aftermath of the severe financial crisis of 2008, and during the groundbreaking intrusion of technological solutions in the insurance and, generally, the financial services sector. Particularly with respect to the financial sector, legislators and regulators aimed to minimize the possibility for any future systemic risks, increase corporate transparency requirements and strengthen consumer protection.⁷ In relation to the data protection field, the different implementation of Directive 95/46/EC across the Member States led to inconsistencies that created complexity, legal uncertainty and increased administrative costs,⁸ and thus the need for reform.

As far as the GDPR is concerned, its enactment and entry into force is considered to be the most significant change in personal data protection law during the last

market players to reform the structure of existing distribution networks that widely consisted up to now of both agents and brokers.

⁵According to the provisions of Directive (EU) 2018/411 that transferred the deadline for the national laws transposing the IDD to be enacted to 1 July 2018, and the date since which said national measures had to apply, to 1 October 2018 at the latest.

⁶Such as the processing of employees’ personal data, the processing of special categories of personal data, any restrictions to the rights granted to data subjects, etc. Such implementing, more detailed provisions, have been adopted, for example in Greece, by virtue of Law 4624/2019, which caused the need for further compliance measures to be taken, in order for the data processing operations to be aligned with the national law provisions as well.

⁷Emond and Tereza (2019).

⁸European Commission – Fact Sheet, *Questions and Answers – Data protection reform*, 21 December 2015, available at: http://europa.eu/rapid/press-release_MEMO-15-6385_el.htm.

20 years,⁹ updating and modernizing the principles of the 1995 Directive. Taking into account the needs that triggered its enactment the main aims of the GDPR, as declared in its text, are on the one hand the provision of adequate protection to individuals, who are expected to gain more control over their personal data,¹⁰ and, on the other hand, the facilitation of businesses with the reduction of the administrative costs.¹¹ At the same time, the GDPR provisions also seem to have taken into consideration the rapid technological developments that have increased the scale of data collection and sharing,¹² and that are expected to further take place and add to the challenges of personal data protection. In this regard, personal data protection obligations are being described in the GDPR provisions in such a generic and broad manner (e.g. with the use of general legal terms, such as “appropriate technical and organizational measures”, reference to the “state of the art”, etc.) that allows their constant adaptation to any further technological advances.

The IDD provisions, on the other hand, were included in the financial services legislative texts that aim at minimizing any future systemic crises from taking place. As such, its main objectives include the minimum harmonization of insurance distribution regulation across the EU, and the enactment of consistent prudential standards and of elevated conduct standards.¹³ At the same time, the IDD operates as a tool aiming to the enhancement of the EU Single Market in the insurance sector, thus, intending to create a level playing field for all different insurance distribution channels,¹⁴ reduce any cross-sectoral differences and improve the competitiveness level of the EU insurance market.¹⁵ Further to the above, the IDD provisions also

⁹Patel (2017).

¹⁰See Recitals No. 10 et. seq. of the GDPR.

¹¹See Recital No. 9 of the GDPR, as well as reference to the benefits of the new provisions in the Communication from the Commission to the European Parliament and the Council, *Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018*, COM(2018) 43 final, 24 January 2018, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563892565511&uri=CELEX:52018DC0043>.

¹²Truli (2016).

¹³PwC, *Hot Topic – Insurance Distribution Directive – Are you ready? – Update February 2018*, PwC, February 2018, available at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=15&cad=rja&uact=8&ved=2ahUKEwjznMqu2MjjAhVQqaQKHWNXCKMQFjAOegQICRAC&url=https%3A%2F%2Fwww.pwc.co.uk%2Ffinancial-services%2Fassets%2Fpdf%2Finsurance-distribution-directive-are-you-ready-january2018.pdf&usg=AOvVaw0GzYf6-KfmQ38U2v5sovEG>.

¹⁴In this context, the scope of the IDD not only covers insurance intermediaries, but also insurance undertakings, when engaging in direct sales to customers – see Article 1(2) in conjunction with Article 2(1)(1) of the IDD.

¹⁵Deloitte, *Insurance Distribution Directive (IDD): the MiFID of insurance*, 2017, available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKEwjznMqu2MjjAhVQqaQKHWNXCKMQFjAIegQIARAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fgr%2FDocuments%2Ffinancial-services%2Fgr_insurance%2520distribution%2520directive_noexp.pdf&usg=AOvVaw2KmAlxEQC4lOigxnILyLXk.

intend to improve consumer protection,¹⁶ providing for enhanced precontractual information and conflicts of interest obligations.

Law and Regulatory Supplements Apart from the main legal texts of the GDPR and the IDD (and their national harmonizing laws), a series of secondary, implementing hard and soft law texts has been adopted to supplement the data protection and insurance distribution regulatory framework. From a data protection law perspective, several Guidelines on specific issues arising from the GDPR provisions¹⁷ had already been adopted by the Working Party of Article 29 (of the Directive 95/46/EC), and have now been endorsed by the newly established European Data Protection Board (EDPB), that continues issuing additional Guidelines, Opinions and other tools concerning the implementation of the GDPR.¹⁸ The GDPR provisions are further supplemented by national law provisions regulating more specific issues, as mentioned above, as well as by virtue of regulatory decisions and guidance issued by the competent national Data Protection Authorities, in a way that the affected insurance market participants still need to take into account any national legal and regulatory particularities that may apply to their operations and which are evolving on an ongoing basis.

Similarly with respect to the IDD, the European Commission has issued (on the basis of relevant authorizations provided in the IDD provisions) delegated¹⁹ and implementing acts²⁰ which regulate specific issues, e.g. more detailed rules on the Product Oversight and Governance (POG) obligations, a standardized template for the Insurance Product Information Document (IPID), etc. Given that the IDD is a minimum harmonization directive (in the sense that Member States may provide for more stringent obligations on insurance distributors), and that its provisions do not (as a rule) apply directly, but need to be harmonized by virtue of national measures, which are the ones applicable, insurers and intermediaries falling into the scope of the new rules will need to examine what national IDD laws they need to comply with, particularly in case they engage in cross-border activities, given that conduct supervision falls into the ambit of the host regulator's supervision.²¹ In parallel,

¹⁶EIOPA, *Annual Report 2016*, published on 15 June 2017, available at: <https://eiopa.europa.eu/publications/annual-reports>.

¹⁷Such as the interpretation and implementation of the transparency notion under the GDPR, the Data Protection Impact Assessment, the Data Protection Officer, the data portability right, etc.

¹⁸See a list of the applicable Guidelines endorsed and/or adopted by the EDPB at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

¹⁹Available at: https://eur-lex.europa.eu/search.html?DB_DELEGATED=32016L0097&qid=1563887687983&DTS_DOM=ALL&type=advanced&lang=en&SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL.

²⁰Available at: https://eur-lex.europa.eu/search.html?qid=1563887688536&DTS_DOM=ALL&type=advanced&DB_IMPLEMENTING=32016L0097&lang=en&SUBDOM_INIT=ALL_ALL&DTS_SUBDOM=ALL_ALL.

²¹In this sense, an insurance distributor established in Germany, but selling insurance in France, will have to comply (for its France-related operations) with the applicable French IDD provisions, and

EIOPA is also empowered and proceeds with issuing soft law guidelines concerning the implementation of IDD provisions, which should be also taken into account.²² As a result, also with respect to the IDD, market participants need to consider any applicable national law and regulatory derogations, in order to ensure their compliance with the new regime.

1.2 *Impact on Insurance Activities*

As noted above, both the GDPR and the IDD radically reform the previously applicable data protection and insurance mediation laws, significantly affecting the operations of both insurance undertakings and intermediaries. The transformation projects undertaken by the affected companies in light of the new rules touch upon and affect all functions, departments and activities, from the ones concerning the relations with customers, business partners and other third-parties, to the ones pertaining exclusively to internal organizational and operational issues.

Internal Effects From an internal aspect, insurers have been required to amend any existing or to adopt new policies and procedures regulating their data collection and processing activities, to identify and implement the appropriate legal bases for each processing activity, to incorporate the privacy by design and by default notions in the procedures and guidelines they follow when designing new activities, to appoint a Data Protection Officer, to conduct data protection impact assessments (when required under the applicable provisions), and to amend their privacy notices and related documentation to customers according to the new information obligations.²³ At the same time, the IDD and its national transposing measures have obliged the affected parties to draft and adopt additional policies and procedures (e.g. POG policies, insurance distribution policies, etc.), to appoint responsible key persons for the insurance distribution activities, and even to proceed with the certification of such key persons and other involved employees.²⁴

with the German IDD provisions with respect to any products it sells in Germany—see in this regard also PwC, *Hot Topic – Insurance Distribution Directive – Are you ready? – Update February 2018*, as above.

²²See in this relevance: <https://eiopa.europa.eu/consumer-protection/insurance-distribution-directive>.

²³See Patel (2017).

²⁴For example in Greece, under the previously applicable law, the employees of insurance undertakings did not need to be certified as to their professional knowledge. According to the Greek law transposing the IDD, the insurance undertaking's employees that are directly involved in the insurance distribution activities, as well as the persons assigned with the responsibility for such activities, have now been required to take exams organized by the Bank of Greece (the Greek Regulatory Authority) and have their professional knowledge and experience certified.

Impact on External Relations With respect to any external relations, insurers have been required to re-evaluate the consent declarations they had been using, and even to request that their customers would grant them anew any necessary consents (or to identify a different, more appropriate legal basis for the processing of personal data). The relations between insurers and intermediaries have also been scrutinized from a data protection law perspective, causing some times debates between the parties, as it was necessary to determine whether they constitute controller-to-processor or controller-to-controller relations, in order to further assess what, if any, GDPR compliance measures needed to be taken.²⁵ The IDD provisions similarly impact on almost all external relations in the context of the insurance business: depending on the exact national law requirements, any cooperation agreements between insurers and intermediaries need to be reexamined and duly amended, to reflect any obligations arising for each party from the new rules. With respect to the distributor-customer relation, the IDD elevates the customer's best interest as an overarching principle, in the sense that the interests of the customers are required to be taken into account precontractually, as customers need to be proposed insurance products which are suitable and appropriate for them at the time of purchase, but also throughout the life cycle of a product.²⁶ In this relevance, insurance distributors are required to prepare appropriate procedures and documentation, to be able to proceed with the specification of the customer's demands and needs, to provide advice concerning an insurance product,²⁷ and to explain the link between the proposed product and the customer's demands and needs.²⁸

Compliance Projects It derives from the above that the entry into force of the GDPR and the IDD regulatory frameworks has caused insurers and intermediaries to engage in long, time-consuming and burdensome compliance projects, which have even gone as far as to completely restructure their operations. Although relating to different policy and law sectors, the GDPR and IDD sets of rules affect each other, and compliance with both these frameworks is intrinsically interconnected: to advise a customer on an insurance product according to the IDD, data collection and

²⁵KPMG, *The GDPR and key challenges faced by the Insurance industry*, February 2018, available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjMg4fw_cjjAhUQKlAKHYK3AHsQFjAAegQIBBAC&url=https%3A%2F%2Fassets.kpmg%2Fcontent%2Fdam%2Fkpmg%2Fie%2Fpdf%2F2018%2F03%2Fie-gdpr-for-insurance-industry.pdf&usg=AOvVaw0bmREPmoGtekQSR5_7t2gz.

²⁶Bernardino (2016).

²⁷Particularly in cases where national laws on IDD render obligatory the provision of advice, in the sense of a personalized recommendation.

²⁸Caroline Veris and Patricia Goddet – Deloitte, *Insurance Distribution Directive – 2018: a challenging year for the European insurance sector*, Performance magazine issue 25, available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjBq6mxvcvjAhVbURUIHfeZBXcQFjAAegQIAhAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fflu%2FDocuments%2Ffinancial-services%2FInsurance%2Fflu-insurance-distribution-directive-2018-challenging-year-european-insurance-sector-012018.pdf&usg=AOvVaw3gvYcV6eDFpDwSB2_x-B7j.

processing needs to take place, thus the relevant procedure needs to take into account the GDPR requirements. The same applies in other aspects as well. Considering that data collection and processing is crucial for the insurance business, in the context of numerous operations ranging from risk assessment and premium calculation to claims payment,²⁹ it is self-evident that any IDD-related compliance actions need to be designed bearing in mind the GDPR requirements and the relevant compliance actions already undertaken.

Such interplay becomes even more evident and the parallel compliance with both frameworks imperative with the expansion of insurance technology (InsurTech) solutions: the use of InsurTech and, particularly, of Internet of Things (IoT) applications in the insurance industry expands and covers all areas from risk assessment to policy and premium re-evaluation and to claims evaluation, and results in an exponential increase of the volume of personal data collected and processed by insurers. In this regard, InsurTech applications need to be designed in a way that safeguards compliance with the applicable data protection principles and requirements in general, but also ensures that any IDD-related requirements (such as the obligation to act in the customer's best interest) are also respected.

This chapter does not aim to exhaustively track down all the possible aspects and cases where GDPR and IDD rules interact, or to propose adequate solutions in the questions which such interaction may pose. Its aim is to highlight some characteristic examples of functions and procedures where such interplay is evident, and lay down some initial thoughts concerning the particular aspects of such interaction that arise and must be taken into account.

2 GDPR and IDD Interaction Affecting Internal Functions

The new data protection and insurance distribution regulatory frameworks establish new, enhanced obligations on the insurers and intermediaries falling into their scope. These cause them to undertake remedial measures affecting first of all their internal organization and operations. The new sets of rules have caused the radical amendment of their internal policies and procedures or the adoption of new ones, the creation of new internal positions and, in general, have added up to the already heavy internal governance obligations that were imposed on the affected parties, particularly on insurers by virtue of the Solvency II regime.

In this relevance, and considering that data collection and processing has always been at the core of the insurance business, any remedial measures aiming to ensure compliance with the IDD provisions shall be also examined as to whether they

²⁹Insurance Europe, *GDPR is around the corner: time for final checks by insurers – An overview of insurers' obligations under the General Data Protection Regulation*, May 2018, available at: <https://www.insuranceeurope.eu/sites/default/files/attachments/GDPR%20is%20around%20the%20corner.pdf>.

encompass personal data processing, in which case, they should be designed and implemented bearing also in mind the applicable GDPR provisions and obligations. All the more so, to the extent that the use of InsurTech solutions that lead to increased volumes of data input to insurers and more direct and frequent insurer-customer interaction and data transmission is integrated in the newly developed functions. At the same time, any GDPR-related compliance measures need to be drafted taking account of the particularities stemming from the nature of the relevant insurance business.

2.1 Product Oversight and Governance Requirements for Manufacturers

One of the characteristic—if not the most characteristic—examples of internal organization obligations described in the IDD³⁰ and its implementing provisions,³¹ with significant interaction with the GDPR-related obligations, are the newly established Product Oversight and Governance (POG) obligations for insurance undertakings and insurance distributors.³² POG requirements constitute one of the most important novelties in the EU insurance distribution regulation enacted by virtue of the IDD, aligning in this respect insurance regulation with the respective provisions already applicable in other financial services sectors.³³ POG arrangements are considered to be part of the company's system of governance (though not being considered as constituting a new key function for insurers³⁴), comprising of internal processes, functions and strategies aiming to ensure a correct design of insurance products, thus intrinsically linked with the Solvency II corporate governance framework and filling a gap thereof from a customer protection point of view.³⁵

³⁰Article 25 of the IDD.

³¹Namely the provisions of the Commission Delegated Regulation (EU) 2017/2358 of 21 September 2017 supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors (the “POG Regulation”).

³²The discussion around the GDPR and the POG-related obligations and their interplay concerns cases where POG-related activities and procedures entail the collection and processing of personal data, and not exclusively of statistical and/or fully anonymized data.

³³Thus constituting a good example of the so-called “Mifidization” of the insurance regulation, as POG requirements were first included in the MiFID II text. See in this respect Prof. Pierpaolo Marano, *The “Mifidization”: The Sunset of Life Insurance in the EU Regulation on Insurance?*, Liber Amicorum for Professor Ioannis Rokas, 2017.

³⁴EIOPA, *Preparatory Guidelines on product oversight and governance arrangements by insurance undertakings and insurance distributors*, EIOPA-BoS-16-071, 18 March 2016, available at: <https://eiopa.europa.eu/Pages/Guidelines/Preparatory-Guidelines-on-product-oversight-and-governance-arrangements-by-insurance-undertakings-and-insurance-distributor.aspx>.

³⁵EIOPA's Preparatory Guidelines on POG, as above.

As described in the applicable provisions, the POG requirements aim to ensure effective customer protection, a level playing field for all market operators, equal conditions of competition and an appropriate standard of consumer protection,³⁶ in line with the general EU insurance regulation objectives of protection of policyholders and beneficiaries.³⁷ In this regard, the intended outcome of effective POG requirements is the correct identification of the target market for each insurance product, as well as the design of more targeted insurance products, better suited for the insurance demands and needs of the respective target market. The design and adaptation, however, of insurance products to their target market, as well as the effective monitoring of insurance products throughout their life span, requires the collection and processing of significant volumes of data, including personal data. Said activities, in their turn, fall directly into the scope of the GDPR, which evidences the interdependence between these two sets of rules.

2.1.1 Product Approval Process

The core POG-related obligations on insurers and intermediaries qualifying as manufacturers of insurance products³⁸ consist in that said manufacturers shall adopt, implement and review an appropriate “Product Approval Process” regulating the development and distribution of new products and significant adaptations to existing insurance products. Such Product Approval Process shall be designed having in mind the principle of proportionality, in the sense that it shall be relatively simple for straightforward and non-complex products, and more complex in case of more sophisticated products that may entail higher risk for the customers.³⁹

The main elements that should be included in a Product Approval Process can be summarized in the definition of: (a) the “insurance product” or the “material change” to an insurance product, (b) the methods used to identify the target market for the insurance product and the risks relevant to said target market, (c) the methods used to determine the appropriate distribution strategy and the information to be provided to the distributors, (d) the methods used to ensure that the insurance product is distributed to the identified target market, and (e) how the insurance product will be monitored and reviewed.⁴⁰

³⁶Recital (1) of the POG Regulation.

³⁷Recital (16) of the Solvency II Directive (Directive 2009/138/EC).

³⁸According to Article 3(1) of the POG Regulation, insurance intermediaries are considered to be manufacturers “*where an overall analysis of their activity shows that they have a decision-making role in designing and developing an insurance product for the market*”, while under par. 2 of the same Article, such decision-making role is deemed to exist if the intermediary autonomously determines the essential features and main elements of an insurance product (e.g. coverage, price, costs, risk, target market, etc.), which are not substantially modified by the insurer providing coverage for the insurance product.

³⁹Recital (2) of the POG Regulation.

⁴⁰BaFin, *Product approval process: Requirements for product manufacturers and distributors*, 02.03.2018, available at: <https://www.bafin.de/dok/10523912>.

Target Market Identification The identification of the appropriate target market and of the demands and needs thereof in the context of the Product Approval Process requires the collection and processing of significant data volumes by manufacturers (Big Data), including personal data. Target markets shall be identified at a sufficiently granular level depending on the characteristics and risk profile of their members, as well as on the complexity and nature of the respective insurance product.⁴¹

A strong trend in the insurance sector towards increasingly data-driven business models, in the context of which traditional data sources (e.g. demographic data, exposure data) are being combined with new sources like IoT-deriving data, online media data, etc., is being documented,⁴² and is expected to impact on the insurance product design procedures and result in better segmentation of the different target markets. Insurers are seen to be taking advantage of the technological advances in order to address any asymmetric information phenomena they have been facing until recently, due to which they were not able to offer insurance products reflecting accurately the risk profile of their customers.^{43,44}

In this relevance, Product Approval Processes are expected to further incorporate in the product design functions the use of new and innovative data sources and Big Data Analytics (BDA) tools, aiming to better understand the customers' needs and characteristics, define further segmented target markets, develop more tailored products and services, and proceed with more accurate risk assessments. The impact of advanced BDA tools has already been evident in this regard, with the appearance and continuous development of usage-based insurance products, particularly in motor and health insurance.⁴⁵

Product Testing At the same time, in the course of the Product Approval Process, and before proceeding with distributing a new insurance product, manufacturers shall test their insurance products appropriately, including scenario analysis, in order

⁴¹Filip Oller, KPMG Luxembourg, *Product Oversight and governance requirements under IDD*, 24 October 2017, available at: <https://blog.kpmg.lu/product-oversight-and-governance-requirements-under-idd/>.

⁴²EIOPA, *Big Data Analytics in Motor and Health Insurance: A Thematic Review*, 2019, available at: <https://eiopa.europa.eu/Pages/News/EIOPA-reviews-the-use-of-Big-Data-Analytics-in-motor-and-health-insurance.aspx>.

⁴³Porrini (2017).

⁴⁴For example EIOPA stated that, in case of motor liability insurance products, which are mandatory for consumers and which may limit product differentiation, require less granularity and detail in terms of the identified target market, while in the case of insurance-based investment products (IBIPs), which are more complex, the identification and description of the appropriate target market should be more detailed.

⁴⁵In this context, and with the integration of IoT tools into the insurance value chain, the process is leading to the identification of insurance demands and needs on a completely individual basis in relation to each customer, and to the design of completely personalized insurance products.

to assess whether the product meets the identified needs, objectives and characteristics of the target market throughout its lifetime. Such product testing operations may need to go, depending on the nature and the characteristics of the product tested, up to the point of testing the product on a pilot group, to examine whether it meets the expectations of the target customers or not,⁴⁶ in which case personal data will once again be collected and processed.

2.1.2 Product Monitoring Phase

Apart from the obligations related exclusively to the design phase of an insurance product, the Product Approval Process shall also provide for and regulate the continuous and regular monitoring of a product launched in the market, with the aim to ensure that it continues meeting the intended customers' demands and needs, and that it does not cause any adverse effects to the customers. In this regard manufacturers shall proceed with regular reviews of the products and identify any factors that may significantly alter the demands and needs or the characteristics of the identified target market, or the main features, the coverage and the guarantees of the insurance product.⁴⁷ In the same context, manufacturers shall document and take account of any circumstances that may adversely affect the customers of an insurance product, and proceed with taking appropriate measures to mitigate such adverse effects, informing at the same time the customers and the distributors of such remedial measures.⁴⁸

All the above mentioned monitoring and review actions that take place in the after-sales service phase, and with a view to being efficient and to truly add to customer protection, as is the aim of the POG obligations, require further collection and processing of personal data determining the exact circumstances that may materially affect the characteristics of the insurance product or the target market, or that may cause adverse effects to the customers. In order to further assist in the collection and evaluation of such data, insurers have also introduced technological tools in the post-sales service and assistance sectors, such as automated answers in their call centers, robotized customer service evaluation, to generate insights about complaint management, fraud detection and customer authentication issues.⁴⁹

⁴⁶EIOPA, *First set of Questions & Answers on the Application of the Insurance Distribution Directive*, 11.07.2018, available at: <https://eiopa.europa.eu/Pages/News/EIOPA-publishes-first-set-of-Questions%2D%2DAnswers-on-the-Application-of-the-Insurance-Distribution-Directive.aspx>.

⁴⁷Article 7(1) of the POG Regulation.

⁴⁸Article 7(3) of the POG Regulation.

⁴⁹EIOPA, *Big Data Analytics in Motor and Health Insurance: A Thematic Review*, as above.

2.2 *Product Distribution Arrangements*

POG provisions impose further obligations on both manufacturers and distributors concerning the distribution of insurance products. The measures to be taken to ensure compliance with said obligations similarly entail data processing issues, in a way that the design and implementation of POG compliance measures needs to take into account any applicable GDPR-related aspects so as to ensure compliance with the respective data protection obligations as well.

2.2.1 *Choice and Audit of Appropriate Distribution Channels*

The identification of the target market by manufacturers under the Product Approval Process impacts upon the choice of the distribution channels to be used, as they must be appropriate for said target market.⁵⁰ The choice of appropriate distribution channels may also entail data collection and processing activities on behalf of the manufacturer, particularly in the event that the affected distributors are individuals, and to the extent that the choice of appropriate distributors is deemed to require the processing of information on the key persons being responsible for the insurance distribution activities.

In the same context, manufacturers provide the distributors with information on their Product Approval Process and the objectives thereof, and ensure that their products are being distributed in accordance with said Process, namely, in accordance with the identification of the target market for each product, i.e. whether the insurance products are being distributed on said target market.⁵¹ Nevertheless, this obligation does not automatically result in a strict prohibition to distributors to sell an insurance product outside the target market, neither does it oblige manufacturers to take any measures against distributors proceeding with such sales, in any case. On the contrary, according to EIOPA's guidance, in cases of distribution outside the target market, manufacturers need to assess whether there are any adverse consequences for the customers outside the target market, who were provided with the product and take corrective measures, in case of such adverse effects, in order to mitigate them.⁵² Such assessment, however, evidently entails personal data collection and processing activities, aiming to assess the possibility for any adverse effects on the specific customers.

⁵⁰Article 8(1) of the POG Regulation.

⁵¹Article 8(3) of the POG Regulation.

⁵²EIOPA, *First set of Questions & Answers on the Application of the Insurance Distribution Directive*, as above.

2.2.2 Product Distribution Arrangements

In terms of distributors, the POG Regulation provides that they shall also have in place specific product distribution arrangements with the aim to ensure that they obtain from the product manufacturer all information required on the specific features of the insurance product and the identified target market, aiming to prevent and mitigate customer detriment, support a proper management of conflicts of interest and ensure that the objectives, interests and characteristics of customers are duly taken into account.⁵³ Furthermore, insurance distributors are required to ensure that the distribution strategies they follow are in line with the distribution strategies and target markets identified by the product manufacturer.

For these objectives to be achieved, insurance distributors will need to collect and process customers' personal data so that they assess whether any conflicts of interest may arise, and to evaluate the customers' characteristics, demands and needs, so that they assess whether each customer falls into the relevant target market, and propose appropriate insurance products. The volume of personal data collected in this context increases exponentially with the use of new technologies (IoT, connected devices), that are being more and more included in the design of new distribution strategies and methods. As such, product distribution arrangements need to be drafted and designed in a way that takes into account the necessary data processing activities for their efficient implementation, as well as any related GDPR (and other data protection) obligations.

Reporting to the Manufacturer The obligations which IDD and its implementing POG Regulation pose on distributors extend throughout the life span of the insurance product. Distributors shall monitor and notify the manufacturer of any indication that the insurance product is not in line with the target market's demands and needs, or in any event that they become aware of any circumstances that may adversely affect the customers.⁵⁴ For distributors to fully comply with these obligations, they shall monitor the performance of the insurance products they distribute during their whole term, by maintaining contact with the relevant customers, and by collecting and processing adequate and appropriate data, that will allow them to duly evaluate the product's performance and conformity with the insurance demands and needs of the identified target market. Should such alignment not occur or cease, distributors will also have to transfer the relevant data to product manufacturers, in order for appropriate measures to be taken. Similar data transfers will have to take place in case of adverse effects caused by or due to product characteristics to the customers.

All the above, indicatively stated, personal data collection and processing activities will have to be duly designed in the product distribution arrangements adopted by insurance distributors, in a way that takes into consideration the GDPR-deriving

⁵³Article 10(1) and (2) of the POG Regulation.

⁵⁴Article 11 of the POG Regulation.

data protection obligations. More to that, the issue of the legal capacity under the GDPR, in which insurance distributors act when processing such personal data and transferring them to the product manufacturers, should be also examined, as further data protection implications may arise, that may even affect the form of the cooperation between the distributors and the manufacturers.

2.3 *Related Data Protection Issues*

As derives from the above brief analysis, compliance with the POG and product distribution obligations requires the design, adoption and implementation of a series of internal policies, procedures and activities that encompass personal data collection and processing and, as such, fall into the scope of the GDPR provisions. In this respect, the design of any appropriate IDD compliance measures should not take place without also taking into account any relevant GDPR implications, and without ensuring compliance with the new data protection framework as well.

2.3.1 *Privacy by Design and by Default*

A key element of the GDPR's risk-based approach and its focus on the accountability principle⁵⁵ is the adopted legal obligation for data controllers⁵⁶ to put in place appropriate technical and organizational measures designed to implement data protection principles, both at the time of the determination of the means for processing and at the time of the processing itself (privacy by design), and for ensuring that, by default, only personal data which are necessary for each specific processing purpose are being processed (privacy by default).⁵⁷ The notion of privacy by design, as the idea of integrating data protection principles at the design of any system, service, product or process, and throughout their lifecycle, is not a new one, as the need to be proactive in considering any privacy requirements has been acknowledged long before the GDPR.⁵⁸ Nevertheless, it was by virtue of the

⁵⁵In the sense that data controllers must ensure and be able to demonstrate compliance with the GDPR provisions.

⁵⁶I.e. of the persons that, alone or jointly with others, determine the purposes and means of the processing of personal data—see Article 4(7) of the GDPR.

⁵⁷Article 25 of the GDPR.

⁵⁸The term “privacy by design” was originally used by Ann Cavoukian, the Information and Privacy Commissioner in Ontario, Canada, and was broken down in the so-called “seven foundational principles”: 1. Proactive not Reactive, Preventative not Remedial; 2. Privacy as the Default Setting; 3. Privacy Embedded into Design; 4. Full functionality—positive sum, not zero sum; 5. End-to-end security—full lifecycle protection; 6. Visibility and transparency—keep it open; 7. Respect for user privacy—keep it user-centric. See in this respect: <https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf>.

GDPR provisions that the privacy by design notion transformed from a “best practice” (as it was considered under the previous regime) to a legal obligation.

General Principles and Guidelines As a legal obligation, the privacy by design and by default notions shall be embedded in the design of all activities that may entail personal data processing operations, including in the design of the Product Approval Processes and the product distribution arrangements of manufacturers and distributors respectively (POG-related obligations, policies and procedures in general), taking into account the nature, scope, context, purposes and complexity of the relevant activities, the state of the art and costs of implementation of any measures, and the risks that the processing operations may cause to individuals. Data controllers shall implement appropriate technical and organizational measures and necessary safeguards, designed to implement the applicable data protection principles in an effective manner and to protect the rights and freedoms of data subjects.⁵⁹

In practice, compliance with the privacy by design and by default principles could be achieved by ensuring that data protection outcomes are achieved, when drafting the POG-related policies and procedures, such as⁶⁰:

- Considering data protection issues as part of the product approval process and product distribution arrangements;
- Rendering data protection an essential component of the above mentioned policies and procedures;
- Ensuring that only the personal data that are needed for the POG-related purposes are being processed⁶¹;
- Ensuring that any IT systems, services, etc. being employed in POG arrangements safeguard personal data protection;
- Disclosing both within and outside the organization the identity and contact details of the persons responsible for data protection (such as the Data Protection Officer);
- Adopting a simple language policy for any public documents, such as the notices explaining to the customers the processing of their personal data for purposes relating to product design and monitoring;

⁵⁹See Guidelines 4/2019 on Article 25, “Data Protection by Design and by Default” of the European Data Protection Board, adopted on 13 November 2019—Version for public consultation, available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf. To be noted that the final relevant guidance of the EDPB on the privacy by design and by default notions, along with practical guidelines for their effective implementation, after the public consultation, was not made publicly available by March 2020.

⁶⁰Information Commissioner’s Office, *Guide to the General Data Protection Regulation (GDPR) – Accountability and Governance – Data Protection by design and by default*, 22.05.2019, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>.

⁶¹For instance, distributors, when designing the procedures for reporting any adverse circumstances to product manufacturers, shall ensure that only the personal data relating to and adequately describing such adverse circumstances will be transferred to the product manufacturers.

- Providing customers/data subjects with appropriate tools, so that they can determine whether their personal data are being properly processed.

As a result, apart from ensuring that the minimum requirements set by the IDD and the POG Regulation are met, insurers and intermediaries shall also ensure that any data processing operations are also taking place in the context of a design process integrating data protection principles in both the design and operational phase thereof. Furthermore, measures to mitigate any risks to the affected individuals, taking into account the state of the art and the cost of implementation, shall be also selected and implemented throughout the POG arrangements; such measures shall be appropriate and effective, in the sense that they must assist the data controller in ensuring and being able to demonstrate compliance with the GDPR. Equally important, the appropriate data protection safeguards shall be implemented into the processing activities described in the applicable POG arrangements.⁶²

Manufacturer—Distributor Relations Taking into account that the privacy by design and by default obligations refer to data controllers, the issue of whether an insurance distributor qualifies as an individual (or joint) data controller or as a data processor acting on behalf of the manufacturer-data controller, and to what extent, becomes of importance even at the stage of designing appropriate and adequate product distribution arrangements. Should the insurance distributor be characterized as a data controller, the case is quite simple as it will bear complete responsibility in embedding privacy by design and by default into its product distribution arrangements. The issue, however, becomes a bit more complicated, in case the distributor is considered to be joint controller with the manufacturer, in the sense that they jointly determine the means and purposes for the processing activities in the context of the product distribution. In this case their cooperation agreement should also contain a specific description of the roles and responsibilities undertaken by each of them in terms of the data protection obligations and, namely, the ones stemming from the rights granted to data subjects by the GDPR, and the ones concerning the provision of appropriate information to them.⁶³ More to that, the possibility for the distributor to be considered to act as data processor⁶⁴ on behalf of the manufacturer (who is acting as the data controller), should also not be precluded, particularly in cases where the distributor does not have any discretionary powers and exclusively follows the guidelines and mandates of the manufacturer when it comes to product distribution activities. In such case, would the distributor as a data processor not have to comply with the privacy by design and by default obligations when designing its product distribution arrangements? Or would the manufacturers, as data controllers,

⁶²European Data Protection Supervisor (EDPS), *Opinion 5/2018 – Preliminary Opinion on privacy by design*, 31 May 2018, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en.

⁶³Article 26 of the GDPR.

⁶⁴I.e. as the person which processes personal data on behalf of the data controller—see Article 4 (8) of the GDPR.

have to ensure that the distributors-data processors they choose to cooperate with design and operate their processes in a way that safeguards personal data protection, thus indirectly obliging distributors to endorse privacy by design and by default principles in any case whatsoever? What additional provisions and safeguards would have to be included in the cooperation agreement between the manufacturer and the distributor, in order to duly reflect such controller-processor relation⁶⁵?

In the same context, issues concerning the privacy requirements implemented by each one of the parties involved and, particularly, any inconsistencies between the different privacy arrangements, should be also identified and addressed, in a way that the different privacy settings are duly respected by all parties, particularly in cases involving BDA. The solution of “automated policy definition and enforcement”, in a way that one party cannot refuse to follow the policy of another party in the same chain, could be examined in this direction.⁶⁶

Third Party Providers Rapid technological advancements and the increasing penetration of InsurTech solutions throughout the insurance value chain impacts the product design phase as well. Product approval and monitoring processes quickly incorporate InsurTech tools, aiming to collect through them the adequate and appropriate data needed to achieve their goals. Although many insurers directly invest in technological research and innovation, others cooperate with InsurTech providers in order to purchase or obtain rights to use appropriate tools. Even in this case, and though InsurTech providers would not directly be seen as falling into the scope of the obligation to abide with privacy by design and by default principles, they would have to (and insurers and intermediaries cooperating with them should examine whether they do) design their products in a way that enables data controllers to implement all necessary measures to ensure data protection.⁶⁷

Privacy-Enhancing Technologies In the same relevance, and as a means to assist them in ensuring the integration of data protection principles into their product approval and distribution arrangements, manufacturers and distributors should consider using privacy-enhancing technologies (PETs), i.e. technologies that embody fundamental data protection principles, by minimizing personal data use,

⁶⁵Particularly in light of Article 28 of the GDPR regulating the controller-processor relationship, and par. (3) thereof, providing for the minimum contractual provisions that shall be included in the agreement or other legally binding document to be executed between them.

⁶⁶ENISA, *Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics*, December 2015, available at: <https://www.enisa.europa.eu/publications/big-data-protection>.

⁶⁷EDPS, *Opinion 5/2018 – Preliminary Opinion on privacy by design*, as above. See also in this relevance Recital 78 of the GDPR, stating that: “When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations . . .”.

maximizing data security, and empowering individuals.⁶⁸ Despite the fact that they have not yet become a standard and widely-used component in system design, PETs such as encryption, protocols for anonymous communications, attribute-based credentials, etc.,⁶⁹ could be incorporated into the product approval and distribution policies designed and implemented in light of the new IDD obligations, ensuring at the same time compliance with the applicable GDPR provisions.

Privacy by Design in Big Data Analytics Product design and monitoring processes in large scale are expected to require the collection and use of big data by product manufacturers, thus giving rise to increased privacy concerns. As a result, increased privacy by design arrangements will need to be integrated in the design and implementation of the relevant product approval and distribution procedures. In this relevance, the notion of “selectiveness” could assist in ensuring GDPR compliance: its accurate implementation would ensure that only the information that is actually needed for a specific analysis is securely being accessed and processed (instead of collecting all possible data to feed the analysis).⁷⁰

Privacy by Default In the same time, the privacy by default notion, as elaborated in the relevant GDPR provisions, is intrinsically linked with the data minimization and the purpose limitation principles,⁷¹ according to which data controllers shall ensure that they process only the personal data required for the specific processing purpose, and that they do not proceed with any further processing of the personal data for purposes other than the specific, legitimate ones they collected the personal data for (which shall be further notified to the data subjects concerned). In this sense, and in order to comply with both the privacy by default obligations, and the obligations to abide by the general processing principles of the GDPR, POG-related arrangements encompassing personal data processing shall be designed in a way that personal data processing is limited to the personal data that are necessary for the correct and sufficiently granular identification of the target market, for the adequate monitoring of the insurance product’s performance, and for no further processing purposes (such as, for example evaluation of a customer’s behavior).

⁶⁸See ICO’s GDPR guidance on privacy by design and by default, as above. ENISA refers to PETs as “software and hardware solutions, i.e. systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons”—see also in this respect: <https://www.enisa.europa.eu/publications/big-data-protection>.

⁶⁹ENISA, *Privacy and Data Protection by Design – from policy to engineering*, December 2014, available at: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

⁷⁰ENISA, *Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics*, as above.

⁷¹As provided in Article 5(1) of the GDPR.

2.3.2 Transparency and Information Issues

Another set of major issues arising from the GDPR provisions and concerning the collection and use of personal data in the course of the implementation of POG-related arrangements, refers to the obligations of data controllers to duly inform the affected individuals of the processing their personal data undergo, in line with the general principle of transparency of the data processing activities.⁷² Transparency constitutes an overarching principle in the GDPR constellation,⁷³ applying irrespectively of the legal basis applicable and throughout the processing activities, to three central areas:

- The provision of information to data subjects related to fair processing of their personal data, i.e. before or at the start of the data processing activity (when the personal data is being collected either from the data subject or otherwise obtained);
- Any communications between the data controllers and the data subjects in relation to their rights under the GDPR, i.e. throughout the processing period; and
- Facilitating the data subjects to exercise their rights, or at other specific points during the processing period, such as when data breaches occur, or in case of other material changes to the processing.⁷⁴

Transparency Concerns in POG Arrangements Personal data processing in the context of product design and product monitoring and evaluation activities, particularly in the cases involving massive data collection through connected devices, or big data analytics, could raise transparency concerns. Traditional notice mechanisms, such as simple privacy notices, written forms, etc., are considered to be inadequate to provide proper transparency and control over the personal data processing activities.⁷⁵ Particularly in the case of BDA tools being employed, the transparency concerns are more elevated, as many firms encounter difficulties in

⁷²As provided in Article 5(1)(a) of the GDPR.

⁷³Although not defined in the GDPR provisions, the notion of transparency is described in Recital 39 of the GDPR, according to which: “It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain information and communication of personal data concerning them which are being processed ...”.

⁷⁴Working Party 29, *Guidelines on transparency under Regulation 2016/679*, 17/EN, WP260 rev.01, adopted on 29 November 2017 and last revised and adopted on 11 April 2018, as endorsed by the EDPB, available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guide-lines-recommendations-best-practices_en.

⁷⁵ENISA, *Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics*, as above.

adequately and properly explaining some complex data processing tools and procedures.⁷⁶

POG arrangements shall be designed so as to ensure that affected data subjects are provided with the appropriate information on the processing of their personal data,⁷⁷ in a way that complies with the transparency requirements.⁷⁸ Namely, any information solutions to be adopted, shall ensure that the information or communication to the data subjects must be concise, transparent, intelligible and easily accessible, using clear and plain language, must be in writing or by other means, including (where appropriate) by electronic means or even orally where requested by the data subject, and generally free of charge. It is crucial, when designing the way of providing the required information, that it is clearly differentiated from any non-privacy related information (such as other precontractual information to be provided under the IDD provisions), and that the necessary information is provided in a way that prevents information fatigue of the individuals. Data subjects must be able to duly determine in advance the scope and the possible repercussions of their personal data processing activities, in a way that they are not surprised at a subsequent stage. However, given that the GDPR increased information obligations add to the existing obligations to provide precontractual information to the customers that derive from the applicable insurance regulation (e.g. the load of information prescribed by the IDD and the Solvency II Directive), the problem of providing overwhelming information to the customers arises, which, in its turn, may lead to opposite results than the intended customer-data subject protection.⁷⁹

Information Obligations In this relevance, insurers and intermediaries are ultimately obliged to think out of the box and manufacture alternative methods and means of providing the required information to the customers. The use of InsurTech solutions throughout the insurance value chain, which grants insurance market players the possibility to develop a direct and continuous relation and communication with their customers could be also employed in order to address any transparency concerns that may arise from encompassing data processing operations into the product design and monitoring procedures to be implemented.

GDPR provisions already grant data controllers the discretion to provide the required information via electronic tools, where appropriate (which could be the case, for example, where customers agree to connect with their insurer by means of connected devices). In such cases, the transparency goals could be achieved by employing not (or not only) plain textual communications, which do not seem to

⁷⁶EIOPA, *Big Data Analytics in Motor and Health Insurance: A Thematic Review*, as above.

⁷⁷As set out in Articles 13 and 14 of the GDPR (depending on whether the personal data are being collected directly from the data subjects or from other sources).

⁷⁸A description of the transparency requirements, in the form of the general rules applying to any information and/or communications to the data subjects, is provided in Article 12 of the GDPR.

⁷⁹Tarasiuk (2019).

adequately and efficiently address the evolution of services,⁸⁰ but also by incorporating into the design of the product offering and monitoring phases layered approaches (which can provide information to the users at different stages of the processing and at different levels of detail), maybe even in combination with standardized icons, pictograms and other visualization tools, which are provided for in the GDPR, where appropriate.⁸¹ In this regard, the integration of technological advances into the adopted POG-related arrangements, should not only aim at increasing the amount and frequency of data input from the customers, but should also be employed in a way that assists in achieving compliance with the GDPR transparency obligations.

2.3.3 Other Privacy-Related Implications

The extensive collection and use of personal data for the purposes of efficient POG arrangements in line with the relevant IDD provisions enhances already existing or triggers new GDPR-related obligations.

Data Protection Impact Assessment According to the GDPR, a Data Protection Impact Assessment (DPIA) is a process designed to describe the processing activity, assess the necessity and proportionality of said processing activity, identify the risks to the rights and freedoms of the affected individuals, and assist in defining the appropriate measures to mitigate said risks. In this relevance, DPIAs are considered to be tools assisting the data controllers with their accountability obligations, as they not only help them comply with their GDPR obligations, but also to demonstrate and prove compliance at any point.⁸² As described in the GDPR provisions, a DPIA is mandatory only in cases the contemplated processing activity is likely to result in a high risk to the rights and freedoms of natural persons,⁸³ particularly when new data processing technologies are employed, and, in any case, in the processing operations the national Data Protection Authorities have included in their lists of processing activities requiring the conduct of DPIAs.

In the case of data processing operations taking place in the course of product design and monitoring activities, they would most likely be considered as triggering the obligation for a DPIA, particularly in case of systematic and extensive evaluation

⁸⁰Indicatively, it was shown that, in order for an average user to read the privacy policies for all visited web services, he/she would need to spend approximately 30 working days per year. See ENISA, *Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics*, as above.

⁸¹Working Party 29, *Guidelines on transparency under Regulation 2016/679*, as above.

⁸²Working Party 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determine whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*, adopted on 4 April 2017, 17/EN, WP 248, and endorsed by the EDPB, available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

⁸³Article 35(1) of the GDPR.

of personal data including automated decision-making processes, large scale processing of special categories of data or even of simple personal data, matching or combination of different datasets, innovative use of technological solutions, or in case the data processing may prevent the data subjects from exercising their rights or using a service/contract.⁸⁴ As a result, the design of the product approval process and the product distribution arrangements, shall be accompanied by a Data Protection Impact Assessment, in accordance with the relevant GDPR provisions and guidance, including at least the following information concerning the relevant data processing activities:

- a systematic description of the processing operations (e.g. nature, scope, context and purposes of the processing, personal data categories, recipients and retention period, functional description of the processing activity, etc.);
- an assessment of the necessity and proportionality of the processing activity (e.g. identification of the measures taken contributing to the necessity and proportionality, and to the rights of the data subjects, including definition of specified, legitimate and explicit purposes, data minimization measures, etc.);
- identification of the risks to the rights and freedoms of the data subjects concerned (e.g. reference to the origin, nature, particularity and severity of the risks, to the potential impacts to the data subjects, etc.);
- identification of the appropriate measures envisaged to mitigate the above mentioned risks; and
- reference to any third party involvement and input to the DPIA (e.g. advice of the DPO, views of the data subjects or their representatives, etc.).

Depending on the data activities envisaged in the course of the product approval, distribution and monitoring arrangements, and on the severity of the risks to the data subjects that may arise thereof, the risk mitigating measures may not be considered to sufficiently reduce the potential risks from the envisaged processing activities. In such case, manufacturers or distributors (as the case may be) will have to consult with the competent Data Protection Authority before launching the contemplated data processing activities, which may even conclude that said processing activities shall not take place at all.⁸⁵

Further to the above, if the product design, distribution and monitoring activities deem to require a DPIA, such Assessment shall take place primarily at the design stage of such processes. However, the DPIA, as well as the compliance with all GDPR obligations, is not prescribed as an one-off exercise, but rather as a

⁸⁴These data processing activities are included in the indicative examples of operations that trigger the obligation for a DPIA according to Article 35(3) of the GDPR, the WP 29 Guidelines on DPIA, while most of these categories have been included in the lists of activities triggering the DPIA obligations, issued by the national Data Protection Authorities—see, indicatively, the relevant list issued by the Hellenic Data Protection Authority (HDPa) in its Decision 65/2018, published in Government Gazette B' 1622/10.05.2018, available at: https://www.dpa.gr/portal/page?_pageid=33,239286&_dad=portal&_schema=PORTAL.

⁸⁵The provisions of Article 36 of the GDPR are of relevance.

continuous exercise that has to be repeated regularly, in order to ensure continuous compliance of the relevant data processing activities with the GDPR provisions.⁸⁶ In the context of such regular review and re-evaluation as to the adequacy of the DPIA findings, the measures taken to mitigate any risks to the data subjects may also have to be duly updated, in line with the state of the art developments.⁸⁷

Data Protection Officer The GDPR provisions establish a new position in the organizational structure of data controllers and processors, the Data Protection Officer (DPO), the appointment of whom is obligatory in case the core activities of the data controller/processor consist of processing operations, which require large scale, regular and systematic monitoring of data subjects, or large scale processing of special categories of personal data.⁸⁸ Insurance undertakings, given the significance of data collection and processing activities for their insurance business, are among the categories of data controllers falling into the scope of the obligation to appoint a DPO. Such obligation is further enhanced in the event that additional data processing activities are designed to be included in the functions of the insurance company, in the course of its product design, distribution and monitoring activities. The DPO, as described in the relevant GDPR provisions,⁸⁹ monitors the compliance of the company with its GDPR obligations, and shall be involved, from the earliest stage possible in all issues relating to data protection, including where a DPIA is being carried out.⁹⁰ As such, the manufacturer's and/or the distributor's DPO (as the case may be), shall be included in the design of the product approval, distribution and monitoring arrangements, so that he/she may identify the privacy-related issues that may arise therein, and assist the company in ensuring compliance with the related GDPR obligations.

Records of Processing Activities Under the GDPR provisions, data controllers are obliged to maintain records of the data processing activities they undertake in writing (including in electronic form), which shall be made available upon request to the competent Data Protection Authority.⁹¹ In this respect, the data processing operations taking place in the course of the product design, distribution and monitoring functions, shall be also duly recorded in such records, which shall contain references to the processing purposes, the categories of the personal data and data subjects involved, the categories of recipients to whom personal data are being disclosed,

⁸⁶Working Party 29, *Guidelines on Data Protection Impact Assessment (DPIA) and determine whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, as above.

⁸⁷Bieker et al. (2017).

⁸⁸See in this relevance the provisions of Article 37 of the GDPR.

⁸⁹Articles 38–39 of the GDPR.

⁹⁰Working Party 29, *Guidelines on Data Protection Officers (DPOs)*, adopted on 13 December 2016, last revised and adopted on 5 April 2017, 16/EN, WP 243 rev. 01, as endorsed by the EDPB and available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

⁹¹See Article 30 of the GDPR in this relevance.

where applicable information on any cross-border data transfers to countries outside the EEA, the envisaged retention periods for the different data categories, and a general description of the adopted technical and organizational security measures being implemented.

The new IDD framework on insurance distribution provides for new internal governance obligations on both insurers and insurance intermediaries falling into its scope. Such new obligations include the need for insurance manufacturers to adopt and implement appropriate Product Approval Processes, which may also provide for procedures to effectively monitor the performance of the insurance products being released in the markets, while insurance distributors shall similarly adopt and implement appropriate product distribution arrangements. Taking into account the goals which these new procedures aim to accomplish, in terms of defining appropriate and sufficiently granular target markets for the insurance products depending on the characteristics, the demands and needs of the respective customers, and ensuring that the products are duly distributed in the relevant target market, and continue being aligned with the insurance demands and needs without causing any adverse effects to the customers, as well as the fact that data collection and processing has always been of utmost importance for the development of insurance business, it becomes self-evident that product design, distribution and monitoring requires corresponding and extensive data collection and processing operations. As a result, compliance with the relevant IDD obligations must be designed and achieved in a way that compliance with the applicable GDPR obligations is at the same time ensured.

In this relevance, the privacy by design and by default notions and their practical implications should be taken particularly into account during the design of the relevant POG-related policies and procedures, in the sense that the GDPR data processing principles (especially the principles of data minimization, purpose limitation and data safety) shall be embedded into the new policies, as an integral part thereof. Particularly in case of the use of InsurTech and BDA tools, any transparency concerns shall be properly and adequately addressed, in order to ensure that the data subjects are aware of the nature, scope and consequences of the data processing activities that concern them, and are not taken by surprise at a subsequent stage. Technological advances should be employed aiming to further enhance the transparency factor, where and as appropriate. The design and implementation of the new POG-related operations shall be duly monitored as to its compliance with the GDPR by the company's appointed DPO, while a DPIA seems to be obligatory before and during the course of the new or enhanced data processing activities. The details of such processing activities should be also duly documented, in records of data processing activities having the minimum content prescribed in the relevant GDPR provisions.

3 GDPR and IDD Implications in the External Relations

The IDD provides for elevated conduct obligations on insurance distributors, aiming to an enhanced level of customer protection. In this context, and in order to duly comply with the obligation to always act in the best interest of the customers, insurance distributors are legally obliged to collect and process personal data of their customers (and potential customers), so that they may identify such best interest and act accordingly. As already discussed, such conduct obligations extend—from a time perspective—not only at a pre-contractual stage, but also throughout the term of the relationship with the customer. In this relevance, compliance with said IDD-deriving obligations needs to be designed and implemented bearing in mind the GDPR-related obligations that may ensue.

At the same time, the cooperation between insurers and intermediaries requires, under the relevant IDD provisions, the exchange of information containing personal data, thus creating further data protection challenges. The definition of the exact nature of the relationship between insurers and intermediaries in light of the applicable GDPR provisions also poses crucial questions that may affect their cooperation as a whole. Similarly, IDD and GDPR provisions have the potential to affect the relations between competitors, creating new questions.

3.1 *Relations with Customers*

The IDD provisions, aiming to achieve the main goal of strengthening consumer protection attribute a key role to the principle of transparency governing insurance distribution by tightening the rules on information provided by insurance distributors, providing for obligations concerning information duties, conflicts of interest, disclosure of remuneration systems, etc.⁹² The effective and full compliance with these obligations requires either the disclosure of personal data to the customers, or the collection and processing of personal data from the customers, in the various stages of the distributor—customer relation.

3.1.1 **Choice of Insurance Product: Risk Assessment**

The general principle applicable on the relationship between insurance intermediaries and their customers under the IDD constellation is that intermediaries shall always act having in the mind the best interest of their customers.⁹³ In this context, distributors are required to determine the insurance demands and needs of their customers, on the basis of the information received from them, and always propose

⁹²Malinowska (2016).

⁹³Article 17(1) of the IDD.

an insurance contract that is consistent with such identified demands and needs,⁹⁴ while in case advice⁹⁵ is provided to the customer in relation to an insurance product,⁹⁶ the distributor shall also explain the reasons why the proposed insurance product is better suited for the customer. The obligations to duly explain to the customer the reasons why the proposed insurance product fits their demands and needs intend to further enhance the transparency in the insurance distribution process, to the benefit always of the customer. Particularly in the case of cross-selling, the above mentioned identification of demands and needs must result in proposing a bundle of products that better suits the customer as a whole.⁹⁷

In this context, the IDD compliance measures to be taken, shall be designed in a way that ensures the adequate identification of the customer's insurance demands and needs and of the appropriate insurance product to be offered. Any product distribution arrangements outlining the steps to be taken up to the proposal of a specific insurance product to the customer, shall determine the information that needs to be provided by the customer, the means to be used in this context, and the way in which the collected information will be translated into specific insurance demands and needs. However, also with a view to the customer relations of the company, given that such identification of each customer's particular characteristics requires the collection and processing of personal data, the design and implementation of such procedures will need to take into account the applicable GDPR obligations. Namely, also these relevant procedures will have to be drafted in accordance with the privacy by design and by default principle, ensuring particularly that only the personal data required to achieve the specific processing purpose of determining the customer's insurance demands and needs are collected, and that such data are not subject to any further processing. Furthermore, the relevant distribution arrangements will also need to be designed in a transparent way, in the sense that the customers will have to be provided with all the required information on the relevant processing of their personal data. Distributors will also need to define the appropriate legal basis for the processing of such personal data, depending mainly on whether any special categories of personal data are being collected.⁹⁸

⁹⁴Article 20(1) of the IDD.

⁹⁵In the sense of a personalized recommendation to the customer.

⁹⁶To be noted that national legislators have taken advantage of the discretion provided by the relevant IDD provisions and have rendered the provision of advice obligatory in certain cases. The Greek Law 4583/2018 transposing IDD, for instance, provides that all insurance distributors are obliged to provide advice to their customer, with respect to all insurance products (except from large risk insurance).

⁹⁷As determined in Article 24(6) of the IDD.

⁹⁸In which case, according to Article 9 of the GDPR, more stringent conditions will apply, in order for the distributors to be able to duly establish the legitimate collection and processing of such special categories of personal data.

The Case of Insurance-Based Investment Products IDD⁹⁹ and its implementing provisions¹⁰⁰ contain more stringent obligations on distributors that sell insurance-based investment products (IBIPs). Namely, the distribution of IBIPs shall be based on a suitability and appropriateness assessment of the proposed IBIP for the specific customer. The relevant IDD provisions state that the distributor shall seek additional information on the customer's particular characteristics, such as information on the customer's knowledge and experience on the investment sector, on his/her financial status, including his/her ability to suffer losses,¹⁰¹ on his/her investment goals and risk tolerance level,¹⁰² etc., in order to have a reasonable basis for determining that their personal recommendation to the customer meets his/her investment objectives (including his/her risk tolerance), as well as his/her financial situation (including the ability to suffer losses), and is such that the customer has the necessary knowledge and experience in the investment field relevant to the specific type of product or service. It is beyond any doubt that the suitability and appropriateness assessment required in the case of IBIPs distribution entails a significant amount of personal data processing activities, which shall be designed and performed in a way that respects the GDPR provisions as well, as described above. To be noted, however, that fragments of the fundamental GDPR data processing principles have already been included in the provisions of the IBIPs Regulation, according to which it must be ensured that the level of information collected shall be appropriate to the specific type of product or service being considered for the specific customer, in line with the data minimization principle of the GDPR. In this regard the privacy by design and by default notions shall be complied with during the design of the appropriate compliance measures with the IBIPs-related IDD provisions, not only because of the GDPR obligations, but even because of the IDD obligations themselves.

Risk Assessment and Premium Calculation When examining which is the most suitable insurance product to be proposed to each customer, distributors shall also undertake the respective risk assessment exercise, in the sense that they shall evaluate the relevant parameters of each case and evaluate the risk to be undertaken, so that the appropriate premium is also charged.¹⁰³ National insurance laws already

⁹⁹Chapter VI, Articles 26–30 of the IDD.

¹⁰⁰Namely the provisions of the Commission Delegated Regulation (EU) 2017/2359 of 21 September 2017 supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to information requirements and conduct of business rules applicable to the distribution of insurance-based investment products (the “IBIPs Regulation”).

¹⁰¹Such as information on the source and extent of the customer's regular income, assets (including liquid assets), investments and real estate property, and regular financial commitments—see Article 9(3) of the IBIPs Regulation.

¹⁰²Such as information on the length of time for which the customer wishes to hold the investment, his/her preferences regarding risk taking, the risk profile, and the purposes of the investment—see Article 9(4) of the IBIPs Regulation.

¹⁰³See Persatuan Insurans Am Malaysia, *How will I be assessed and what is risk profiling?*, 2019, available at: <http://www.piam.org.my/phased-liberalisation-section/how-will-i-be-assessed-risk-profiling/>.

acknowledge the need for the risk to be insured to be properly and adequately known beforehand to the insurer by providing for precontractual information obligations on the prospective policyholders as well.¹⁰⁴ With respect to the new IDD obligations on distributors, the risk assessment and premium calculation exercise is a crucial part in the procedure towards providing sound advice to their customers in relation to the ultimately proposed insurance product and, as such, the procedures and means for this evaluation shall be designed in line with the overarching IDD principle of bearing the customer's best interest in mind.

In this regard, risk assessment and even risk profiling is a procedure requiring the collection and processing of personal data, both on the insurance history of the customer, and on the current conditions. Distributors are able to take advantage of the new technological advances, such as the IoT, and use the possibilities being offered by connected devices to have access to a significantly large volume of data, so that they may better understand the individual risk profile of each customer, and align their proposals accordingly. The integration, however, of such advances into the risk assessment operations, must take place in a way aligned with the GDPR principles; distributors must carefully determine the personal data they need, to proceed with an accurate risk analysis, and collect from the customers the data that is appropriate, adequate and necessary for such purposes, in line with the data minimization principle. The use of connected devices is going to result in a significantly increased inflow of personal data, which the insurers must be duly prepared, not only to appropriately collect, but also to duly process, for the purposes for which it was collected.¹⁰⁵ In this regard, appropriate safeguards will also need to be implemented, in order to ensure that no further processing takes place, unless the customers—data subjects have been duly informed for any additional processing purposes and such further processing takes place lawfully and according to the GDPR provisions.

3.1.2 Precontractual Information Obligations

Another area where the IDD and the GDPR provisions interact and affect the relation between distributors and their customers is the issue of the precontractual information to be provided to the customers, so that they may make a duly informed decision on the insurance contract to be executed.

Information Overload The IDD provisions aim as already mentioned above, to enhance customer protection. To that end, they require for extensive precontractual

¹⁰⁴For example, the Greek Insurance Contract Act (ICA – Law 2496/1997) in its Article 3 provides that the policyholder shall disclose to the insurer, before the conclusion of the contract, any and all information and circumstances he/she is aware of that are objectively material for the assessment of the risk, while adverse results are provided for the case that the policyholder does not comply.

¹⁰⁵Cindy Maïke, *Insurance risk assessment in a connected world*, 09.01.2019, Horton Works, available at: <https://hortonworks.com/blog/insurance-risk-assessment-in-a-connected-world/>.

information to be provided to the customers, in due time before the conclusion of the contract, concerning the identity and other capacities of the distributor, the specific characteristics of the insurance product being offered, etc. In this respect the IDD has introduced the Insurance Product Information Document (IPID), in relation to non-life insurance products. The IPID is a short, standardized document which conveys the minimum critical information on the insurance type, the insurance cover, the premiums to be paid, the exceptions from the cover, etc.¹⁰⁶ In this regard, the IDD provisions have significantly added to the already existing precontractual information obligations under other insurance regulatory texts, such as the Solvency II and the PRIIPs Regulation¹⁰⁷ in terms of the products falling within its scope, while in case of consumer insurance products, additional information obligations arise from the applicable EU consumer protection Directives¹⁰⁸ and their national implementing measures. The GDPR provisions further add to the above mentioned information obligations, as they oblige distributors to disclose to their customers a significant number of information concerning the personal data being processed, the processing purposes, the data recipients, the legal bases of the processing the customers' rights under the GDPR, etc. From this point, the interplay between the IDD and the GDPR provisions, which both aim, at the bottomline, at the effective protection of the individuals (in their capacity as insurance customers and data subjects at the same time), puts such protective goal at risk. Customers are being overwhelmed with information, which simply becomes confusing, with the effect that their ability to be properly informed and make appropriate decisions when purchasing insurance products may be obstructing.¹⁰⁹

¹⁰⁶The IPID's specific standardized form and content has been elaborated in the Commission Implementing Regulation (EU) 2017/1469 of 11 August 2017 laying down a standardized presentation format for the insurance product information document (the "IPID Regulation"). With respect to the IPID, its very limited size, in combination with the information it needs to contain under the IDD and the IPID Regulation provisions, have caused significant problems to insurers at the implementation phase, as they could not design the IPID in a way compliant with all its requirements. For example, in case of insurance products with multiple covers, insurers were required to determine and choose which covers would be considered to be the "main" ones and be included in the IPID, and which ones not, in a way that could be deemed to be arbitrary.

¹⁰⁷Regulation (EU) No 1286/2014 of the European Parliament and of the Council of 26 November 2014 on key information documents for packaged retail and insurance-based investment products (PRIIPs).

¹⁰⁸Such as the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), or the Directive 2002/65/EC of the European Parliament and of the Council of 23 September 2002 concerning the distance marketing of consumer financial services and amending Council Directive 90/619/EEC and Directives 97/7/EC and 98/27/EC.

¹⁰⁹See a relevant analysis in Insurance Europe, *Submission to the online REFIT Platform tool on information overload, duplication and paper requirements*, October 2017, available at: <https://www.insuranceeurope.eu/submission-online-refit-platform-tool-information-overload-duplication-and-paper-requirements>.

Conflicts of Interest The information to be provided to the customer at a precontractual stage include, among others, information on possible conflicts of interest between the distributor on the one hand and the customer on the other. From a general point of view, the IDD provides that intermediaries shall inform the customer of any close links they may have with an insurer, or of any exclusive cooperation.¹¹⁰ Particularly with respect to the distribution of IBIPs, distributors shall establish and implement an effective conflicts of interest policy, aiming to identify the circumstances that constitute or may result in such a conflict, and to determine the procedures to be followed and measures to be adopted in order to manage such conflicts of interest and prevent them from harming the customers,¹¹¹ including notifying the customer of any particular conflict of interest that may arise.¹¹² In the context of ensuring that customers are duly informed of any potential conflicts of interest causes, the IDD provisions oblige distributors to inform their customers on the remuneration they receive in relation to the insurance product they propose. Particularly insurers proceeding with insurance distribution activities are obliged to inform the customers of the nature or, in some cases, of the actual relevant remuneration their employees shall receive. This aspect of the IDD compliance requirements may not entail (or not exclusively refer to any) any further processing of customers' personal data, but does entail personal data processing in terms of disclosing personal data of the distributor and its employees (as the case may be) to the customers. As such, any IDD compliance measures shall be also designed and implemented in a way that respects and ensures compliance with the applicable GDPR provisions: for instance, any personal data disclosure shall not extend beyond the data necessary for the purpose of complying with the relevant IDD obligations, while the data subjects concerned (e.g. employees, directors, etc.) shall be duly informed of the relevant data processing activities.

3.2 *Relations with Other Insurance Market Players*

The IDD and the GDPR provisions are changing the relationship between the insurance distributors and their customers, both aiming to enhance the level of trust towards the insurance market. At the same time, issues are similarly arising from the interplay of the IDD with the GDPR provisions, with regard to the relations between the different participants in the insurance value chain.

¹¹⁰Article 19 of the IDD.

¹¹¹See Articles 3–8 of the IBIPs Regulation for more details on the particular obligations of the distributors in relation to the prevention and management of the conflicts of interest.

¹¹²Which may concern the customer and any “relevant person” of the insurance distributor, such as a director, partner, manager, employee or other natural person; for a detailed definition of the “relevant person” notion for the purposes of conflicts of interest management in the IDD constellation, see Article 2(1) of the IBIPs Regulation.

3.2.1 Insurer: Intermediary Relation

In the course of the insurance distribution process, the effective cooperation between insurers and intermediaries requires significant data processing activities, namely, exchange of personal data from one to another, throughout the life cycle of the insurance contract. At a precontractual stage, intermediaries are required to collect adequate and appropriate data from the prospective customer and transfer them to the insurer, so that the latter may proceed with the necessary risk assessment exercise, decide whether to accept the risk or not, and properly calculate the proposed premium. During the term of the insurance contract, insurers and intermediaries are required, under the POG-related provisions, to monitor the performance of the product in order to determine whether it continues being in line with the target market's characteristics, while intermediaries shall notify the insurer (i.e. product manufacturer) of any circumstances falling to their attention, that may adversely affect the customer, and the insurer in its turn shall inform the intermediary of any measures taken to duly address such circumstances. Similarly, in case of any risk occurrence event, intermediaries are required to act in the best interest of their customers, collecting and forwarding to the insurer any personal data required for the due satisfaction of the insurance claim.

In the course of the above described activities, intermediaries are seen as collecting and transferring to insurers the necessary personal data for the drafting, conclusion, monitoring and execution of the insurance contract, as such activities are also described in the IDD provisions. In most of the occasions, such collection and transfer of data takes place on the basis of standardized forms and means established by the insurer and made available to the intermediaries the insurer cooperates with for the distribution of its products. Such scheme of collection and transfer of personal data, apart from the need to be designed and implemented to comply with the IDD provisions, also needs to take into account the relevant GDPR obligations.

The major question that arises in this regard is the capacity under which each party operates and, particularly, whether the intermediary will be considered as acting as data processor on behalf of the insurer—data controller, or if the intermediary acts as an independent data controller on its own accord, or if both cases could be applicable—up to a point each one. The delimitation between these concepts is of paramount importance, as it is the data controller that is mostly responsible to ensure compliance with the GDPR provisions, while the data processor only needs to comply with limited provisions of the GDPR applicable directly to it. Furthermore, under the GDPR constellation, should a controller-processor relationship seem to exist, the insurer-intermediary cooperation in terms of personal data activities will have to be regulated under a legally binding agreement, containing specific content, while the insurer as a data controller will be able to give

documented instructions to the intermediary,¹¹³ but will also bear responsibility for any data processing activities undertaken by the intermediary on its behalf. The issue of the delimitation between the notion of controller, as the person actually determining the purposes and means of the data processing activities, and of processor, given its complexity and the vast number of grey areas that apply,¹¹⁴ has caused many controversies between intermediaries and insurers in the course of the GDPR compliance projects undertaken, and still remains to be resolved and its practical implications to be seen.

3.2.2 Relations Between Competitors

Some of the new obligations and tools under the IDD and the GDPR provisions may also potentially affect the relationship between insurance distributors, regardless of their capacity as insurers or intermediaries. The most characteristic example of the way in which the new frameworks may cause issues is the combination of the IDD obligation to propose an insurance product that suits the particular characteristics of the customer, with the data portability right under the GDPR.

According to the newly established data portability right,¹¹⁵ customers have the right (under the conditions prescribed in the applicable provisions) to request that a distributor provides them with their personal data they have provided to the distributor, in a structured, commonly used and machine-readable format, or that the distributor transfers such personal data directly to another distributor. In this regard, a distributor, in the course of collecting the necessary information on a potential customer, in order to determine his/her insurance demands and needs, could ask from said customer to make use of the right to data portability, and provide the distributor with all personal data from another distributor. Such request could possibly mean that the first distributor is required to provide to the new distributor information that could contain personal data concerning the customer but created by the first distributor (such as a complex insurance profile created by compiling raw data). In this respect, such a request would cause the first distributor to embark in a complex exercise in order to determine which personal data they are obliged to provide to the customer (or directly to the new distributor), and which ones they may withhold.¹¹⁶ The outcome of such exercise, however, cannot preclude beyond any

¹¹³Which could go up to the point of requesting that the intermediary deletes all personal data and any copies thereof concerning a specific customer or categories of customers, thus, interfering directly with the intermediary's clientele.

¹¹⁴Some guidance and criteria on the delimitation of these two notions are found in the Working Party 29, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN WP169, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm.

¹¹⁵Under Article 20 of the GDPR.

¹¹⁶Guidance concerning the personal data that would fall into the ambit of such obligation and the ones that could be exempted can be found in the Working Party 29, *Guidelines on the right to data*

doubt the disclosure of commercial secrets from one distributor to another, such that may grant the new distributor an unjustified competitive advantage against the other.

The new IDD and GDPR provisions and the interaction between these two sets of rules impacts the activities throughout the cycle of the insurance distribution: from a precontractual stage up to the satisfaction of any insurance claims. Alongside the new policies and procedures that need to be adopted and implemented, the new insurance distribution and data protection frameworks impact upon the relations between the insurance distributors and their customers, but also between distributors themselves. Compliance with the IDD obligations to propose products that are in line with the customer's individual characteristics, as well as to continuously monitor the product's performance and alignment with their insurance demands and needs, has increased the amount of personal data that need to be collected and processed. As such, the relevant IDD compliance measures need to be designed under the privacy by design and by default principles, taking also account of the other applicable GDPR provisions.

Similarly, the new rules give rise to novel or newly arising issues concerning the relations between insurers and intermediaries. The matter as to whether an intermediary may be characterized as data controller or processor may seem to be a typical, bureaucratic one, but its practical implications are of utmost importance for both parties, as they touch upon the issue of who does the insurance clientele *belong* to. At the same time, compliance with some IDD obligations, such as determining the insurance profile of a customer, may be achieved more easily by taking advantage of some possibilities provided under the GDPR provisions. However, new issues may still arise as to the extent up to which it will be ethical and in line with the honest transactional practices to make use of such new tools, and from what point onwards they could result in distorting the competition between insurance distributors.

4 Summary and Conclusions

The GDPR and the IDD, along with their EU and national implementing provisions, Guidelines, etc., have radically transformed the previously applicable laws on data protection and insurance mediation/distribution, aiming to address shortcomings and deficiencies of the respective previously applicable laws, and to enhance the protection provided to individuals and insurance customers respectively. Such changes impacted on the functioning of the private insurance market in the EU altogether, in some cases causing structural modifications in the market and the cooperation between market players. Furthermore, the need to ensure compliance with the new rules has significantly disrupted the operations of both insurers and intermediaries.

portability, 16/EN WP 242 rev. 01, adopted on 13 December 2016 and last revised and adopted on 5 April 2017, endorsed by the EDPB, and available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

Their almost simultaneous adoption and entry into force triggered some lengthy, time and resources consuming, and burdensome compliance projects that interact with each other in numerous occasions, as the compliance measures concerning the implementation of the IDD provisions need to take into account the requirements set out in the GDPR provisions as well.

GDPR and IDD remedial measures affect first of all the internal operations and functions of insurers and intermediaries, adding to the already extensive corporate governance requirements, as they have caused the amendment and/or adoption of policies and processes (either explicitly provided in the new rules, or implicitly required for compliance with them), the establishment of new key functions and roles in the organizational structures, etc. The Product Oversight and Governance (POG) requirements constitute one of the most characteristic examples where the required IDD compliance measures entail the adoption of extensive data collection and processing operations. The identification of the appropriate target market on the basis of the particular insurance characteristics of its members, the design of insurance products targeting specific insurance demands and needs, and the continuous monitoring of their performance and alignment with the targeted demands and needs require the analysis of increasing data volumes. At the same time, determining the appropriate distribution strategy for each target market, and notifying the product manufacturer of any potential adverse effects the product may cause to consumers, similarly consist of data processing activities. In this regard, any IDD compliance measures have to be designed also in the light of the GDPR obligations, particularly taking account of the privacy by design and by default notions.

In the same way, the new IDD and GDPR provisions affect the relationship between insurance distributors and their customers, between insurers and intermediaries, and even between distributors themselves (i.e. operating in the same level of the insurance value chain). In terms of the relations with their customers, insurers are required under the IDD provisions to always act in the best interest of their customers, determine their insurance demands and needs and ensure that any product they propose suits them, while there are national transposing laws rendering obligatory the provision of advice, in the sense of a personal recommendation. In this regard, IDD compliance throughout the life cycle of the distributor-customer relation requires extensive personal data collection and processing and, thus, needs to be designed and implemented bearing in mind the need to also ensure compliance with the applicable GDPR obligations. As far as the relations between distributors are concerned, IDD provisions require in several cases the exchange of information, including personal data, between them, in a way that triggers the question of the capacity in which each party acts: is the distributor a data processor acting on behalf of the manufacturer or not? And, if yes, to what extent? What would be the practical implications of each response in terms of managing the clientele and the related personal data? At the same time, the use of new GDPR tools may assist in ensuring compliance with IDD obligations, but could raise new issues between insurance distributors when acting as competitors in the market, as it could lead to the disclosure of sensitive commercial secrets of one competitor to another, granting as such competitive advantage to the latter.

The GDPR and the IDD impact on the operation of insurers and intermediaries should not be seen exclusively as two separate procedures and issues to be tackled. The interaction between these two new sets of rules is evident in all relevant aspects, as any measures aiming to the compliance with one of them shall take into consideration and duly integrate the requirements of the other one, in a way that compliance with them is safeguarded as well. The need to combine the requirements of both the GDPR and the IDD into the remedial actions undertaken often constitutes a complex exercise, requiring the cooperation of different functions of the organization. To that end, the rapid integration of technological developments, namely new InsurTech solutions, into the insurance value chain and the daily operations of insurance distributors should be the focal point of this intricate combination of the data protection and insurance distribution requirements, as they may provide assistance to market participants in ensuring their full compliance in the most efficient way.

References

- Bernardino G (2016) Exploring new horizons for the benefit of the citizens in the European Union. In: Keynote and Welcome Speech, EIOPA 6th Annual Conference, Frankfurt. Available at: <https://eiopa.europa.eu/Publications/Speeches%20and%20presentations/2016-10-18%20EIOPA%20Annual%20Conference.pdf>
- Bieker F, Friedewald M, Hansen M, Obersteller H, Rost M (2017) A process for data protection impact assessment under the European general data protection regulation. In: Conference Paper, 4th Annual Privacy Forum, Frankfurt/Main, Germany. Available at: https://www.researchgate.net/publication/319276698_A_Process_for_Data_Protection_Impact_Assessment_under_the_European_General_Data_Protection_Regulation.
- Deloitte (2017) Insurance Distribution Directive (IDD): the MiFID of insurance. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&ved=2ahUKEwjznMqu2MijAhVQqaQKHWNXCKMQfjAlegQIARAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2Fdeloitte%2Fgr%2FDocuments%2Ffinancial-services%2Fgr_insurance%2520distribution%2520directive_noexp.pdf&usq=AOvVaw2KmAlxEQC4IOigxnILyLXk.
- Emond I, Tereza K (2019) European Union regulation of insurance industry in the aftermath of the financial crisis. *Lawyer Q Int J Legal Res* 1(2) Available at: <https://tlq.ilaw.cas.cz/index.php/tlq/article/view/330/336>
- European Commission (2015) Fact Sheet, Questions & Answers – Data protection reform, 21.12.2015. Available at: http://europa.eu/rapid/press-release_MEMO-15-6385_el.htm
- European Commission (2018) Communication to the European Parliament and the Council. In: Stronger protection, new opportunities – Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018, 24.01.2018. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1563892565511&uri=CELEX:52018DC0043>
- Insurance Europe (2017) Submission to the online REFIT Platform tool on information overload, duplication and paper requirements, October 2017. Available at: <https://www.insuranceeurope.eu/submission-online-refit-platform-tool-information-overload-duplication-and-paper-requirements>
- Insurance Europe (2018) GDPR is around the corner: time for final checks by insurers – An overview of insurers' obligations under the General Data Protection Regulation, 05.2018. Available at: <https://www.insuranceeurope.eu/sites/default/files/attachments/GDPR%20is%20around%20the%20corner.pdf>.

- KPMG (2018) The GDPR and key challenges faced by the Insurance industry, 02.2018. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjMg4fw_cjjAhUQKlAKHYK3AHsQFjAAegQIBBAC&url=https%3A%2F%2Fassets.kpmg%2Fcontent%2Fdam%2Fkpmg%2Fie%2Fpdf%2F2018%2F03%2Fie-gdpr-for-insurance-industry.pdf&usg=AOvVaw0bmREPmoGtekQSR5_7t2gz
- Maiké C (2019) Insurance risk assessment in a connected world, 09.01.2019, Horton Works. Available at: <https://hortonworks.com/blog/insurance-risk-assessment-in-a-connected-world/>
- Malinowska K (2016) Insurance transparency and protection regime under the Insurance Distribution Directive. Insurance Review 4/2016. Available at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjztv6fu9LjAhUDwqYKHexAB1AQFjAAegQIABAC&url=https%3A%2F%2Fpui.org.pl%2Fwp-content%2Fuploads%2F2017%2F05%2FWU-2016-04-06-Malinowska-en.pdf&usg=AOvVaw1x7RazC-YDA5le4xFKCQpH>
- Marano P (2017) The “Mifidization”: The Sunset of Life Insurance in the EU Regulation on Insurance? Liber Amicorum for Professor Ioannis Rokas, NOMIKH BIBAIOHKH, Athens, pp. 219–234
- Oller F, KPMG Luxembourg (2017) Product Oversight and governance requirements under IDD, 24.10.2017. Available at: <https://blog.kpmg.lu/product-oversight-and-governance-requirements-under-idd/>
- Patel C (2017) GDPR: main points of the law and its impact on insurance. LexisNexis. Available at: <https://blogs.lexisnexis.com/insurance-insights/2017/08/gdpr-main-points-of-the-law-and-its-impact-on-insurance/>
- Persatuan Insurans Am Malaysia (2019) How will I be assessed and what is risk profiling? Available at: <http://www.piam.org.my/phased-liberalisation-section/how-will-i-be-assessed-risk-profiling/>
- Porrini D (2017) Regulating Big Data effects in the European insurance market. Insur Mark Comp 8 (1) Available at: https://www.researchgate.net/publication/324084745_Regulating_Big_Data_effects_in_the_European_insurance_market
- PwC (2018) Hot Topic – Insurance Distribution Directive – Are you ready? – Update February 2018. Available at: <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjznMqu2MjjAhVQqaQKHWNXCKMQFjAOegQICRAC&url=https%3A%2F%2Fwww.pwc.co.uk%2Ffinancial-services%2Fassets%2Fpdf%2Finsurance-distribution-directive-are-you-ready-january2018.pdf&usg=AOvVaw0GzYf6-KfmQ38U2v5sovEG>
- Tarasiuk A (2019) Consumer insurance – recent regulatory tendencies. In: 20th AIDA Serbia Conference Proceedings, “Insurance Law and Practice – Current Trends, Future Challenges”
- Truli E (2016) The General Data Protection Regulation and civil liability, MPI Oct. 21-22, 2016
- Veris C, Goddet P—Deloitte (2018) Insurance Distribution Directive – 2018: a challenging year for the European insurance sector. Performance magazine issue 25. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjBq6mxvcvjAhVbURUIHfeZBXcQFjAAegQIAhAC&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fflu%2FDocuments%2Ffinancial-services%2Finsurance%2Fflu-insurance-distribution-directive-2018-challenging-year-european-insurance-sector-012018.pdf&usg=AOvVaw3gvYcV6eDFpDWSB2_x-B7j

Regulatory Guidance and Decisions

- BaFin (2018) *Product approval process: Requirements for product manufacturers and distributors*, 02.03.2018, available at: <https://www.bafin.de/dok/10523912>

- EIOPA (2019) *Big Data Analytics in Motor and Health Insurance: A Thematic Review*, available at: <https://eiopa.europa.eu/Pages/News/EIOPA-reviews-the-use-of-Big-Data-Analytics-in-motor-and-health-insurance.aspx>
- EIOPA (2018) *First set of Questions & Answers on the Application of the Insurance Distribution Directive*, 11.07.2018, available at: <https://eiopa.europa.eu/Pages/News/EIOPA-publishes-first-set-of-Questions%2D%2DAnswers-on-the-Application-of-the-Insurance-Distribution-Directive.aspx>
- EIOPA (2017) *Annual Report 2016*, 15.06.2017, available at: <https://eiopa.europa.eu/publications/annual-reports>.
- EIOPA (2016) *Preparatory Guidelines on product oversight and governance arrangements by insurance undertakings and insurance distributors*, EIOPA-BoS-16-071, 18.03.2016, available at: <https://eiopa.europa.eu/Pages/Guidelines/Preparatory-Guidelines-on-product-oversight-and-governance-arrangements-by-insurance-undertakings-and-insurance-distributor.aspx>
- ENISA (2015) *Privacy by design in big data – An overview of privacy enhancing technologies in the era of big data analytics*, 12.2015, available at: <https://www.enisa.europa.eu/publications/big-data-protection>
- ENISA (2014) *Privacy and Data Protection by Design – from policy to engineering*, 12.2014, available at: <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>
- European Data Protection Board (2019) *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default – Version adopted for public consultation*, 13.11.2019, available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf
- European Data Protection Board (2018) *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version adopted after public consultation*, 12.11.2019, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf
- European Data Protection Supervisor (2018) *Opinion 5/2018 – Preliminary Opinion on privacy by design*, 31.05.2018, available at: https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en
- Hellenic Data Protection Authority (2018) *Decision 65/2018 – List of activities requiring DPIA*, Government Gazette B' 1622/10.05.2018, available at: https://www.dpa.gr/portal/page?_pageid=33,239286&_dad=portal&_schema=PORTAL
- Information Commissioner's Office (2019) *Guide to the General Data Protection Regulation (GDPR) – Accountability and Governance – Data Protection by design and by default*, 22.05.2019, available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>
- Information and Privacy Commissioner of Ontario (2018) *Privacy by design – seven foundational principles*, 01.2018, available at: <https://www.ipc.on.ca/wp-content/uploads/2018/01/pbd.pdf>
- Working Party 29 (2017a) *Guidelines on transparency under Regulation 2016/679*, 17/EN, WP260 rev. 01, 29.11.2017 (revised 11.04.2018), available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en
- Working Party 29 (2017b) *Guidelines on Data Protection Impact Assessment (DPIA) and determine whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679*, 17/EN, WP 248, 04.04.2017, available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en
- Working Party 29 (2016a) *Guidelines on Data Protection Officers (DPOs)*, 13.12.2016 (revised on 05.04.2017), 16/EN, WP 243 rev. 01, available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Working Party 29 (2016b) *Guidelines on the right to data portability*, adopted on 13.12.2016 (revised on 05.04.2017), 16/EN, WP 242 rev. 01, available at: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

Working Party 29 (2010) *Opinion 1/2010 on the concepts of “controller” and “processor”*, 00264/10/EN, WP 169, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.