UDC 004.056.53

Influence of EU general data protection regulation for marketing in Ukraine

Drokina N.I.
Candidate of Economic Sciences,
Associate Professor of Marketing Department
of State University of Telecommunications

In the article, the role of General Data Protection Regulation in the world, as well as for marketing in enterprise is shown. The characteristics of the main directions that affect the GDPR policy are given, examples of the consequences of violation of this policy by different companies are given. The role of Ukrainian enterprises in the implementation of the GDPR is considered. The influence of GDPR on the changes in the work of the marketing department is shown. The sequence of the main stages of the marketing strategy is developed taking into account the requirements of the GDPR.

Keywords: General Data Protection Regulation (GDPR), Data protection officers, Data Permission, National Supervisory Authority, marketing strategy.

Дрокіна Н.І. ВПЛИВ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ЩОДО ЗАХИСТУ ДАНИХ ЄС НА МАРКЕТИНГ В УКРАЇНІ
У статті показана роль Загального регламенту щодо захисту даних в світі, а також для маркетингу підприємств. Дана характеристика основних напрямів, які зачіпає політика GDPR, наведено приклади наслідків порушення даної політики різними компаніями. Розглянуто роль українських підприємств в реалізації GDPR. Показано вплив GDPR на зміни в роботі відділу маркетингу. Розроблено послідовність основних етапів маркетингової стратегії з урахуванням вимог GDPR.

Ключові слова: Загальний регламент щодо захисту даних (GDPR), співробітники із захисту даних, дозвіл на використання даних, національний наглядовий орган, маркетингова стратегія.

Дрокина Н.И. ВЛИЯНИЕ ОБЩЕГО РЕГЛАМЕНТА ПО ЗАЩИТЕ ДАННЫХ ЕС НА МАРКЕТИНГ В УКРАИНЕ
В статье показана роль Общего регламента по защите данных в мире, а также для маркетинга предприятий. Дана характеристика основным направлениям, которые затрагивает политика GDPR, даны примеры последствий нарушения данной политики разными компаниями. Рассмотрена роль украинских предприятий в реализации GDPR. Показано влияние GDPR на изменения в работе отдела маркетинга. Разработана последовательность основных этапов маркетинговой стратегии с учетом требований GDPR.

Ключевые слова: Общий регламент по защите данных (GDPR), сотрудники по защите данных, разрешение на использование данных, национальный надзорный орган, маркетинговая стратегия.

Formulation of the problem. New services and technologies become data centered. Collecting, storing, reviewing, transferring or otherwise processing personal data in a secure and lawful way poses an increasing challenge for businesses today. Comprehensive knowledge about data processing regulations is essential to comply with privacy and data protection matters on a national, European and global level. The websites you use, the calls you make, the places you visit and even the photos you take are all recorded, measured and leave a digital footprint – a footprint that is fast becoming a prized resource. In May 2017, The Economist [1] called personal data "the world's most valuable resource" ahead of oil, because of how much it now informs the way companies communicate with their customers and how it positively impacts customer experience [2]. However, because personal data is so valuable, it is vulnerable to theft or misuse and this has led to consumers demanding to know how companies use and store their personal data. This is because, overall, consumers are not convinced companies are doing enough to protect them. A 2016 Consumer Privacy study by TRUSTe/NCSA [3] found that 92% of online customers cite data security and privacy as a concern. While, according to a report published by the Chartered Institute of Marketing [4], 57% of consumers do not trust brands to use their data responsibly.

Another concern is that Symantec's State of European Privacy Report [5] found that 90% of businesses believe it is too difficult to delete customer data and that 60% do not have the systems in place to help them do so. Clearly, there is significant disconnect between consumers, their personal data and how the companies that collect it, use it (fig. 1).

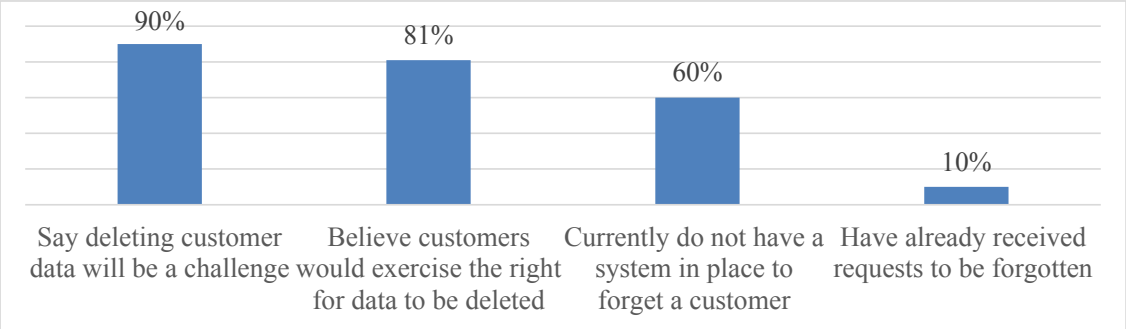

Figure 1. Challenges organizations face if customers ask to have their data modified or deleted

It is even more concerning when it comes to GDPR for marketing as 41% of marketers admit to not fully understanding both the law and best practice around the use of consumer's personal data. The people that *use* customer data the most do not fully understand *how* they should use it. It is clear that something needs to be done to regulate the management of personal data, to protect consumer interests and police the companies that collect, store and use the data. This is why in 2018, the European Union introduced GDPR – a new set of laws designed to safeguard personal data and inform the decisions of marketers in all member states [6]. It also concerns Ukrainian companies both conducting their activities on the EU territory as well as selling goods to EU citizens and residents.

Analysis of recent researches and publications. There are publications at the international and national level regarding this issue, such as Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data dated 1981 (the "Convention") and the 2001 Additional Protocol. In Ukraine all basic information are presented in the law of Ukraine "On Personal Data Protection" (No. 2297 VI, dated 1 June 2010) (the "Data Protection Law"), which is the key legislative act regulating data protection in Ukraine. The Data Protection Law contains similar provisions to those in the Convention. Both the Convention and the Data Protection Law came into force on 1 January 2011. Conceptual principles of GDPR and the basic principles of GDPR are also set out in the scientific works of Steven MacDonald [2; 6; 10; 14], Jennifer Lund [12], Brad Kostka [13], Cathrine Davis [19], Bob Yelland [21], etc. In the articles of these scholars, different issues were raised, such as impact of the GDPR to the company, steps in preparing for the General Data Protection Regulation, risks and companies rights. Still, the open questions of using the concept of GDPR in the marketing activities of enterprises in Ukraine are not sufficiently investigated.

Formulation of the problem. The aim of this research is to determine the basic tendencies of GDPR implementation in marketing department and define the most efficient marketing data protection strategy for Ukrainian enterprises.

Presentation of the main research material. The General Data Protection Regulation (GDPR) is a new digital privacy regulation that was introduced on the 25th May, 2018. It standardizes a wide range of different privacy legislation's across the EU into one central set of regulations that will protect users in all member states.

This means companies will now be required to build in privacy settings into their digital products and websites – and have them switched on by default. Companies also need to regularly conduct privacy impact assessments, strengthen the way they seek permission to use the data, document the ways they use personal data and improve the way they communicate data breaches. Moreover, because it is a regulation and not a directive, it is legally binding – meaning it cannot be opted out of, or ignored. In fact, failing to comply could lead to fines of up to €20 million or 4% of your global turnover [7]. Therefore, it is fair to say that the EU is taking this extremely seriously.

GDPR is 'the most far-reaching change to data protection in a generation' and is a dramatic shift in the way the EU wants personal data to be managed. The EU's new approach to online privacy puts individuals first, believing they should be protected and empowered, rather than exploited or ignored.

This new approach to data protection is the EU's way of keeping companies big and small more accountable for their actions. EU regulators believe that companies have been exploiting personal data for their own gain and aren't being transparent about how they were using it.

GDPR has been designed to end all that and put the power back in the hands of the consumer.

The main reason for introducing this now is that the current EU data privacy regulations are still based on a document that was first adopted in 1980 (later updated in 1995) [8]. This means that the data privacy principles that the EU works are outdated on don't include considerations for social media, smartphones, or even advanced web technology (i.e Artificial Intelligence, Virtual Reality, etc). In addition, the current regulation is only a directive, so companies (and countries) could easily opt-out. From 25th May, 2018 this has no longer been the case [9].

While consistency in data privacy regulations across Europe should be good news for all marketers, GDPR also comes with quite a few challenges that affect marketing teams – especially marketing teams that communicate to customers based in the EU.

On the surface, GDPR might seem extreme, especially for smaller businesses or solo-practitioners. Realistically though, there are only tree key areas that marketers need to worry about – data permission, data access and data focus [6] (tabl. 1).

The deadline for GDPR was passed and many businesses was already in "panic mode" to make sure they're compliant. The trouble with this is that this leads to mistakes. Especially as the Information Commissioner's Office (ICO) has started to clamp down even harder on the misuse of personal data.

In fact, the ICO has already reported three incidents that involve household brand names who tried to use well-known email activation strategies [10] to reach out to their database. The campaigns, which were sent out by Flybe, Honda and Morrisons, asked customers if they wanted to be contacted by email and to update their preferences. They contacted them by email – even those customers that had previously opted out (tabl.2).

These three examples should act as a clear warning sign to businesses – both big and small [6]. Ukraine is not a member state and it may seem that EU regulations and directives are not applicable here. However, GDPR is very different. When it comes to GDPR, anyone outside the EU should be aware of its extra-territorial applicability since it applies to companies anywhere in the world, which come into contact with EU citizens' data.

Ukrainian companies often deal with European Union citizens' personal data. For instance, when developing a SaaS platform for a restaurant or a vet clinic, software developers get access to personal data of people who sign up (waiters, doctors, or pet owners). According to the GDPR, getting access to any personal data, even if this data is not stored on any device, means personal data processing.

Businesses in Ukraine are, in general, quite skeptical about privacy or personal data protection as this area was neglected for many years through inadequate regulation and enforcement. However, below are a few good reasons why businesses in Ukraine should care about the GDPR or even comply with it (tabl. 3).

Global brands across the nation are gearing up for a major change to the data protection and privacy landscape as we know it. Set forth by the European Union, a new piece of legislation known as the General Data Privacy Regulation (GDPR) will transform the way organizations collect and store data. This will have a large impact on Ukrainian companies that operate on a global scale. Namely, marketers

Table 1

Main areas for marketers' considerations in GDPR

Area	Main issues for marketers
1. Data Permission	Data permission is about how need to manage email opt-ins –people who request to receive promotional material from company. In practice, this means that leads, customers, partners, etc. need to physically confirm that they want to be contacted. So, no marketing communication is to be sent out to the referee's email address.
2. Data Access	The right to be forgotten has become one of the most talked about rulings in EU Justice Court history. It gives people the right to have outdated or inaccurate personal data to be removed. The introduction of the GDPR offers individuals a method to gain more control over how their data is collected and used – including the ability to access or remove it – in line with their right to be forgotten. Marketer will be responsibility to make sure that users can easily access their data and remove consent for its use.
3. Data Focus	Marketers need to focus on the data they need. Otherwise, avoid collecting any unnecessary data and stick with the basics.

of these global brands will need to implement new processes and tools that prompt consumers to give explicit consent when sharing their information.

In the marketing department, three roles will see the biggest change in their everyday work (fig. 2) [12].

Although its parameters are extensive, the GDPR ultimately aims to protect the data privacy rights of consumers by holding organizations to higher standards of transparency, security and accountability when it comes to the way they collect and store data. Any companies that fail to comply with these regulations will face significant penalties of up to €20 million or 4% of their global annual revenue, whichever is greater. In order to ensure compliance, global organizations should take proactive steps over the coming months to align their marketing practices with this new regulation.

The GDPR will inevitably transform the marketing industry as a whole – and, with its implementation only months away, global brands should take heed. It will force marketers to ditch tired, old-school tactics and rethink their approach to marketing.

Successful brands will use this as an opportunity to better cater to their consumers by putting more creative and thoughtful marketing practices into play. Initiating a transparent marketing strategy that adds value, not irritation, to consumers' lives will ultimately gain the trust of consumers and drive more success for business.

The five key ways that marketing strategy will be impacted under the GDPR can be identified [13] (tabl. 4).

GDPR does sound intimidating and the fines issued by the ICO are enough to make you rethink your entire marketing strategy [14]. But, in reality, this new legislation isn't a set-back. In fact, it's a great opportunity for company to do what marketers do best – that is create targeted marketing campaigns with people that are engaged with company brand.

In January 2017, Osterman Research, Inc [15] published a paper and found that 73% of businesses are not ready to satisfy the compliance obligations of the GDPR. While a 2016 study by Symantec [16] found that 23% of businesses feel they will only be partly compliant by the May 2018 deadline.

It is very important for marketing department to prepare to GDPR, so the eight main stages of marketers preparation for new data protection conditions at the enterprise can be distinguished (fig. 3).

Here the checklist that includes nine practical tips to create efficient marketing strategy:

1. Audit the mailing list. According to a study by W8 data [17], up to 75% of marketing databases have become obsolete from GDPR and only 25% of existing customer data meets GDPR requirements. Therefore, need to remove anyone where the marketer does not have a record of opt-in. For new subscribers, need to make sure that the potential subscriber confirms that he or she wants to join the mailing list by sending an automated email to confirm the subscription.

2. Reviewing the way of collecting personal data. If the company is buying mailing lists, now might be the time to start fresh with a new mailing list. In the UK, pub chain JD Whetherspoon

Table 2

Examples of penalties for violation of GDPR rules

Company	Incident description	Result
Flybe	In August 2016, Flybe sent an email to 3.3 million people in their database with the subject line "Are your details correct?" It sounds like a smart strategy in theory, but unfortunately, these 3.3 million people had previously opted out (unsubscribed) to marketing emails and thereby gave no consent to be contacted.	£70,000
Honda Motor Europe	In a separate incident, Honda Motor Europe sent an email to 289,790 subscribers between May and August 2016 asking their database "would you like to hear from Honda?" This email was sent in order to clarify how many of the 289,000 subscribers would like to receive marketing emails going forward. But, once again, this email was sent to individuals who had specifically opted out.	£13,000
Morrisons	In late 2016, UK supermarket chain Morrisons re-launched their "Match & More" loyalty program. In a bid to get more members to take advantage of their offers, they sent out an email to all 230,000 members from their database, asking subscribers to update their account preferences. Unfortunately, this included 131,000 subscribers who had previously opted out and unsubscribed.	£10,500

Table 3

Reasons why businesses in Ukraine should care about the GDPR

Reason	Descriptions
1. Ukraine will adopt the GDPR – the only question is when	Ukraine is committed to becoming a member of the European Union. It has signed the *EU–Ukraine Association Agreement*. In terms of the agreement, the parties have agreed to cooperate on the introduction of the highest European and international data protection standards, including ones included in the Conventions of the Council of Europe. When the agreement was signed back in 2014 the wording "the highest European data protection standards" was probably somewhat vague. But now it is clear, because these standards and best practices have been codified in the form of the GDPR. As a prospective member of the European Union, Ukraine has an obligation to approximate its legislation to the legislation of the European Union. Ukraine has already adopted a number of EU Directives and Regulations, so it would only be logical to include the GDPR in the next batch. Taking into account the current dynamics of EU integration processes in Ukraine, the adoption of the GDPR in Ukraine will likely take place during the next two to four years.
2. Early compliance with the GDPR might be more cost effective	The GDPR introduces two concepts, Privacy by Design and Privacy by Default, which change the way modern business should treat personal data and build business processes. Under these concepts controllers have to ensure that the privacy of individuals is considered from the outset of each new processing, product, service or application, and that, by default, only minimum amounts of personal data as necessary for specific purposes are collected and processed. For the past year and a half, many European companies have allocated significant resources, costs and applied efforts to bring their personal data processing activities into line with the GDPR. In general, it is estimated that the process of rearranging processes in line with the GDPR would require around three to six months from a medium-size organization. Therefore, wiring the concepts indicated by the GDPR early, during development of new businesses or business processes, may help businesses in Ukraine to achieve both cost savings and compliance with the GDPR.
3. Some businesses in Ukraine need to comply with the GDPR from May 2018	The GDPR has expanded the territorial scope of its applicability to companies located outside the EU. The GDPR applies to the processing of personal data by controllers and processors outside the EU, where their processing activities relate to the offering of goods or services (even for free) to data subjects within the EU, or to the monitoring of their behavior. Sometimes Ukrainian businesses do not offer goods or services or monitor the activities of data subjects within the EU directly, but rather process personal data at the request of their EU partners (i.e., act as processors). The GDPR imposes compliance obligations directly on processors, such as implementing security measures, notifying the data controller of data breaches, appointing a DPO (if applicable) and maintaining records on processing activities. To improve the enforcement and accountability of a controller or processor not established in the Union (excluding businesses in Ukraine) that processes personal data of data subjects who are in the EU or offers goods or services to EU data subjects, the GDPR establishes a requirement to designate a representative in the EU to act on its behalf with regard to its obligations under the GDPR. Therefore, all businesses in Ukraine, whether controllers or processors involved in the aforementioned activities, should comply with the GDPR.
4. For customer-centric companies, the GDPR is an opportunity to excel in customer service and receive new clients	The GDPR introduces a number of new rights for data subjects with respect to their personal data, including the right to data portability (the right to obtain a copy of one's personal data from the controller and have it transferred to another controller), the right to erasure (or the "right to be forgotten"), the right to restriction of processing, and the right to object to certain processing activities (profiling) and to automated processing decisions. There is no doubt that the introduction of these rights requires companies to make certain changes to their infrastructure, consumer services and approach to personal data. However, it is reasonable to assume that if companies comply with the GDPR consumer experience would soon become the new normal, and even the expected level of service would increase (not only in the EU but also in other countries such as Ukraine). Businesses in Ukraine, which excel in implementing these rights would likely see a degree of benefit in terms of new customers, better customer engagement, and higher customer approval rates.

Ending of Table 3

5. The GDPR's provisions incorporate certain best practices that are "a good to have" practice to manage personal data risks	The GDPR introduces a requirement for businesses to appoint a Data Protection Officer (DPO) where (i) the core activities of the controller or processor consist of processing, which requires regular and systematic monitoring of data subjects on a large scale, or (ii) the core activities consist of processing of special categories of data on a large scale. The *Personal Data Protection Law of Ukraine* already requires the appointment of a DPO in cases where sensitive data is processed. Another new requirement of the GDPR for controllers and processors is to prepare and maintain Data Mapping, which would include records of processing activities and maps showing how personal data flows within various territorial and structural divisions of the organization. The performance of Data Protection Impact Assessments (DPIAs, namely risk analysis) is necessary according to the GDPR, where the processing of personal data (particularly when using new technologies), is likely to result in high risk to the rights and freedoms of individuals.
6. Increased fines, along with a data subject-friendly one-stop-shop approach, support compliance with the GDPR	The GDPR harmonizes the tasks and powers of supervisory authorities and significantly increases fines. For major infringements (such as failure to comply with cross-border transfer rules or to obtain the relevant permits), fines can be up to EUR 20 million or, in the case of an undertaking, up to 4% of the total worldwide annual turnover in the preceding financial year. The supervisory authority in the jurisdiction of the main or single establishment of the controller/ processor will be the lead authority for cross-border processing (subject to derogations). This allows the data subject to file a complaint to one supervisory authority only, and such authority will lead the investigation in as many countries as is necessary, coordinating its activities with other authorities [11].

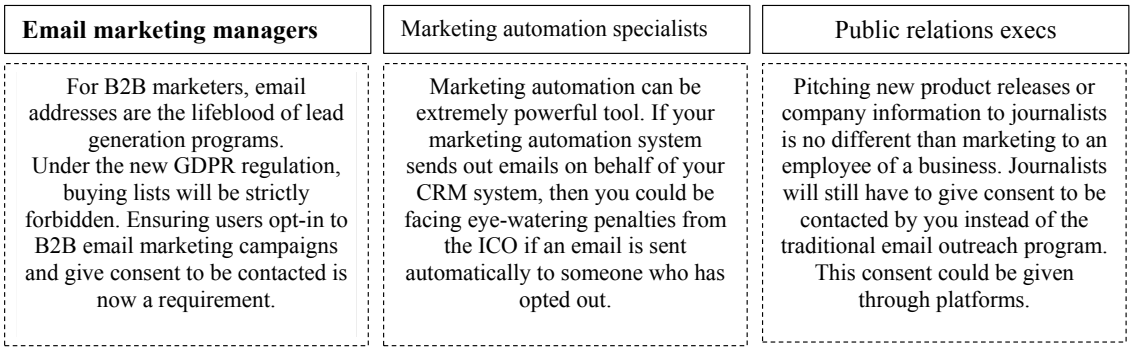

Figure 2. Roles that will see the biggest change after GDPR

[18] took the unprecedented step of deleting their entire email marketing database (more than 650,000 email addresses). In a letter from their CEO, John Hutson informed customers that all customer emails will be securely deleted. While that might be a terrifying prospect for some, it's something to consider as you will then be guaranteed with a list of engaged and interested readers.

3. Investment in a content marketing strategy by creating white papers, guides and eBooks that visitors can access and download in exchange for them sharing their contact information.

4. Invitation visitors to add themselves to the mailing list by launching a pop up on company website. Then the marketer can keep his mailing list neatly segmented by creating specific pop ups for product news, blog posts and general company news.

5. Education of sales team about social selling techniques. Essentially, sales reps should connect with prospects on social media and share relevant content – rather than trying to reach new prospects by email.

6. The time for using Google docs or Excel spreadsheets to store customer data is over. Start centralizing the personal data collection into a CRM system [19]. Need to make sure the users can access their data, review its proposed usage, and make any changes as necessary.

7. Understanding the data, which has been collecting in more detail. When it comes to sign up forms, only ask for what the marketer need, and what he will use. For B2B marketers, full name, email address and company name is usually more than enough.

8. Using push notifications. A push notification is a pop up message that appears on a desk-

top or mobile device. Marketers can use push notifications to send a message to subscribers at any time. However, unlike email marketing campaigns, push notifications do not process personal data (IP addresses are anonymized) and users are required to give explicit consent in order to opt-in and receive notifications.

9. Updating the privacy statement. Marketers need to review the current privacy statement and amend the statement accordingly to comply with GDPR requirements [20].

Conclusions. On 25 May 2018 the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) has replaced the current Data Protection Directive 95/46/EC and will be directly applicable in all EU Member States without the need to implement national laws. The aim of the GDPR is to unify the current patchwork of privacy data regulations that exists in Member States, protect privacy as a fundamental right, and ensure the free flow of personal data between Member States. Adoption of the GDPR has been a result of more than a decade of negotiations, as well as reassessment of privacy as a human right and of personal data as being a value for the economy [21]. There is no doubt that different types of data have become fuel for the modern digital economy, and personal data is one of the most important of all. The availability of data is a strategic enabler for the development of artifi-

Table 4

Five ways the GDPR will impact to marketing strategy

Element	Descriptions of actions with these elements
Lead generation	Generating leads through inbound marketing campaigns will still be possible, but marketers must receive explicit consent from data subjects before collecting any of their personal information. This involves using simplified language to clearly outline what data is being collected and why, then providing a call to action, such as a checkbox, that prompts a user to give informed consent. Pre-checked boxes and automatic opt-ins are prohibited.
Database management	Because a major goal of the GDPR is to hold data collectors to a higher standard of accountability, companies should expect to be monitored for compliance. This means marketers must keep thorough records that demonstrate the data they've collected is accurate and consensual. In addition, they should establish procedures for auditing and maintaining databases to ensure that any contacts without a documented opt-in are removed.
Consumer profiling	Under the GDPR, marketers will be more restricted in what type of data they are allowed to collect —information that is unnecessary, sensitive or related to minors is off-limits. Therefore, the capability to build extremely detailed consumer profiles will scale back to protect the privacy rights of those individuals. At any time, consumers will have the right to revoke their consent and demand their data be deleted.
List-buying and cold emailing	List-buying and cold emailing have been outdated and ineffective for a while. After all, no consumer enjoys being spammed. The GDPR will make it illegal for marketers to contact individuals without their consent, putting an end to these old-school tactics. However, this doesn't mean businesses relying on email marketing for lead generation are doomed. Instead, they have an opportunity to build a better mailing list with an inbound marketing strategy. Rather than buying and/or using email lists, marketers can generate leads by providing valuable content in (consensual) exchange for individuals' email addresses.
Media pitching	The GDPR also will change the way marketers conduct media pitching. For the most part, media pitching is considered a legitimate interest for collecting data under the GDPR as long as it's done in a proper, respectful manner. However, gone are the days where marketers can use the "spray and pray" method of securing media placements. Mass mailings will be strictly prohibited. Although the liability for consent will primarily lie with media databases like Cision and Vocus, marketers need to ensure they don't abuse this data by sending a reporter irrelevant information. Instead, marketers should make sure their media lists are accurate and up to date, take the time to develop genuine, mutually beneficial relationships with the press, and tailor media pitches to each individual reporter.

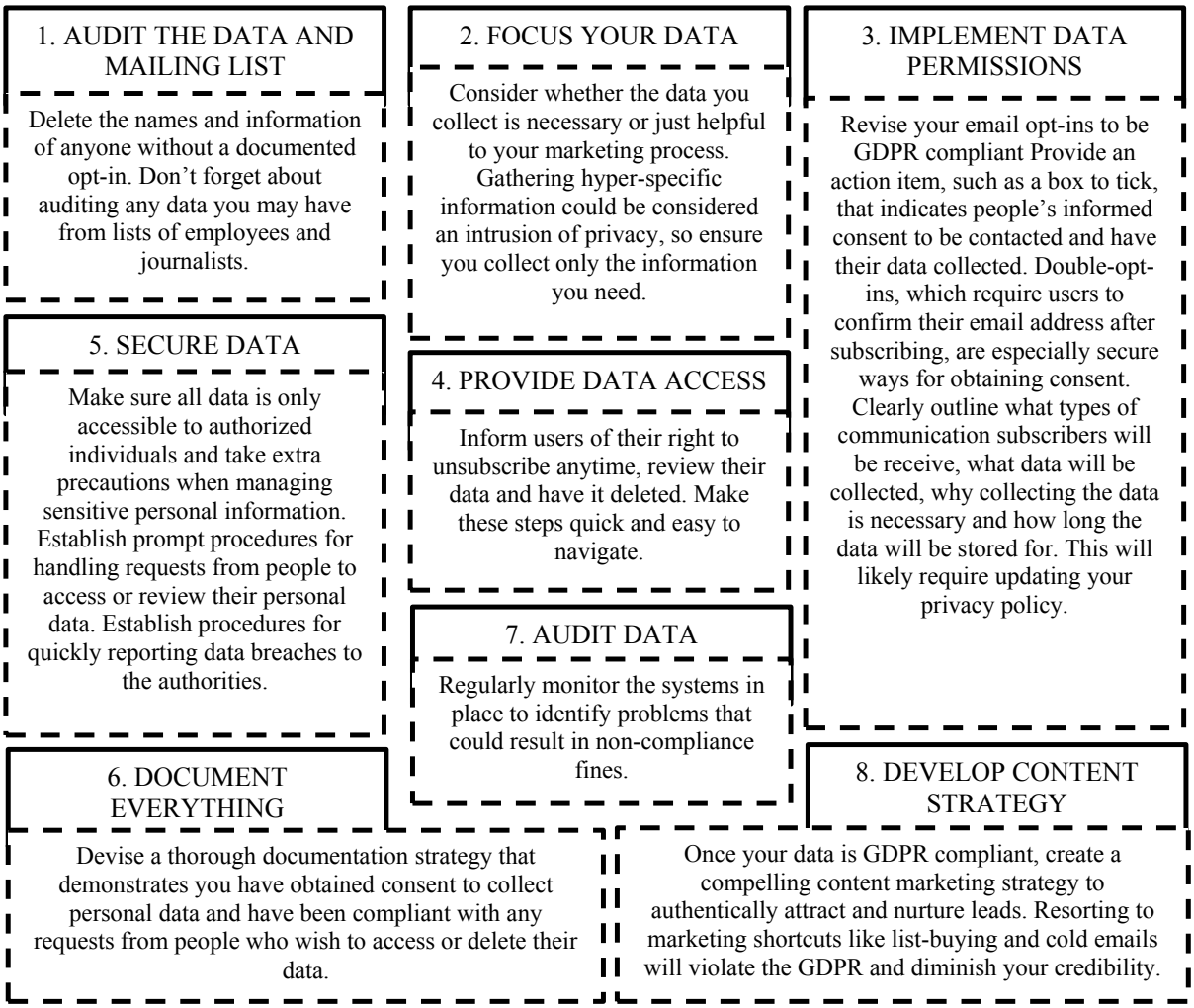

Figure 3. GDPR preparation steps for marketers

cial intelligence, machine learning, big data algorithms and numerous other new technologies. Without proper balancing restrictions, there is a risk that with the help of more and more intrusive technologies, and in the race to acquire this new "gold," businesses may substantially limit privacy as we know it now and use personal data against data subjects for their own advantage. The GDPR addresses these risks and establishes guidelines on how data subjects can maintain control over their data in a digital environment and, at the same time, enjoy all the necessary digital services.

In this regard, it is important to note that businesses in Ukraine will be at a disadvantage compared to their EU counterparts in relation to the soon-to-be introduced GDPR-like regime in Ukraine, because they will likely have less time to prepare, and have historically lower levels of awareness of and compliance with data privacy regulations. Therefore, businesses in Ukraine should move compliance with the GDPR requirements high in their list of their priorities and start organizing the necessary resources, data and expertise to allow an easy transition.

REFERENCES:

1. The world's most valuable resource is no longer oil, but data / The Economist [Electronic resource]: web-site. – Access mode https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

2. 7 Ways to Create a Great Customer Experience Strategy / Steven MacDonald [Electronic resource]: web-site. – Access mode https://www.superoffice.com/blog/customer-experience-strategy/

3. NCSA Consumer Privacy Infographic – US Edition / 2016 TRUSTe [Electronic resource]: web-site. – Access mode https://www.trustarc.com/resources/privacy-research/ncsa-consumer-privacy-index-us/

4. Be transparent on social media or risk the consequences, CIM warns businesses [Electronic resource]: web-site. – Access mode https://www.cim.co.uk/newsroom/opinion-be-transparent-on-social-media-or-risk-the-consequences/

5. Businesses Underprepared for GDPR [Electronic resource]: web-site. – Access mode https://www.symantec.com/en/uk/about/newsroom/press-releases/2016/symantec_1018_01

6. GDPR for Marketing: The Definitive Guide for 2018 / Steven MacDonald [Electronic resource]: web-site. – Access mode https://www.superoffice.com/blog/gdpr-marketing/

7. Article 83. EU GDPR. "General conditions for imposing administrative fines" [Electronic resource]: web-site. – Access mode http://www.privacy-regulation.eu/en/83.htm

8. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Electronic resource]: web-site. – Access mode https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31995L0046

9. EU general data protection regulation – background [Electronic resource]: web-site. – Access mode https://www.dlapiper.com/fi/ukraine/focus/eu-data-protection-regulation/background/

10. How to Use Email Activation Campaigns to Re-engage Inactive Subscribers/ Steven MacDonald [Electronic resource]: web-site. – Access mode https://www.superoffice.com/blog/email-activation-campaigns/

11. Six Reasons Why Businesses in Ukraine should Care about the GDPR [Electronic resource]: web-site. – Access mode http://www.ujbl.info/article.php?id=991

12. How to Create a Revenue Winning Lead Nurturing Strategy / Jennifer Lund GDPR [Electronic resource]: web-site. – Access mode https://www.superoffice.com/blog/lead-nurturing-strategy/

13. Five ways the General Data Privacy Regulation will impact your marketing strategy / Brad Kostka [Electronic resource]: web-site. – Access mode http://www.crainscleveland.com/article/20180306/blogs05/154016/five-ways-general-data-privacy-regulation-will-impact-your-marketing

14. Email Marketing Strategy: A Data-driven Guide (with Original Case Studies) / Steven MacDonald [Electronic resource]: web-site. – Access mode https://www.superoffice.com/blog/email-marketing-strategy/

15. The Impact of the GDPR on Your Business [Electronic resource]: web-site. – Access mode https://ostermanresearch.blog/2017/01/19/the-impact-of-the-gdpr-on-your-business/

16. Symantec – State of European Data Privacy [Electronic resource]: web-site. – Access mode https://www.slideshare.net/symantec/symantec-state-of-european-data-privacy

17. Who are w8data, how can we save you money? [Electronic resource]: web-site. – Access mode https://www.w8data.com/

18. Wetherspoons just deleted its entire customer email database – on purpose [Electronic resource]: web-site. – Access mode http://www.wired.co.uk/article/wetherspoons-email-database-gdpr

19. GDPR and CRM: How to Manage Customer Data in 2018 / Cathrine Davis [Electronic resource]: web-site. – Access mode https://www.superoffice.com/blog/gdpr-crm/

20. GDPR preparation checklist for marketers [Electronic resource]: web-site. – Access mode https://roopco.com/wp-content/uploads/2018/03/GDPR-Preparation-Checklist-for-Marketers.pdf

21. A LITTLE BEE BOOK “How it Works” GDPR Adapted from a variety of sources by Bob Yelland [Electronic resource]: web-site. – Access mode https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=IMM14202GBEN