Digital Marketing Institute

GDPR

Study Notes

GDPR

LESSON 1: KEY CONCEPTS OF GDPR

THE IMPORTANCE OF GDPR

Introduction

In this section, we'll explain the GDPR, some of the key concepts, and how it impacts your work as a digital marketer. We'll look at current guidelines on the GDPR that can help you on this journey and focus on areas that need your special attention.

We'll also discuss some of the main threats to personal data – such as data leaks, personal data becoming out-of-date or unmanageable, misuse, and attacks on your personal data records. In all cases, there are valid commercial reasons that sit behind the requirements of the GDPR.

From a marketer's perspective, this includes building and maintaining trust and keeping the processing of personal data as clean as possible. Each department at your company and organisation will have its own required steps to take to comply with the GDPR in order to mitigate and reduce risk.

At the end of this section, we'll look at the threat to business continuity that can occur because of non-compliance with the GDPR. And it's not just the threat of punitive sanctions and fines imposed by the Supervisory Authority. The bigger threat to business continuity is the potential for damage to brand reputation, the loss of trust and the wider commercial knock-on effects this can have on your company or organisation.

The General Data Protection Regulation

The General Data Protection Regulation is a new law introduced by the European Union on 25th May 2018. Organisations and individuals have had two years to prepare for it since its approval in 2016. The official website states:

> *The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organisations across the region approach data privacy.*

A Regulation is enforceable by law; a Directive is not. Therefore, the GDPR is not optional – it's obligatory if you do business in the European Union or with European Union citizens.

The GDPR:

- Gives individuals more control over the use of their personal data
- Gives clarity across the region on how data can be used from one EU country to the next (and beyond)
- Demands that businesses assign more resources to data privacy, as well as take on more responsibility for it.

Responsibilities of digital marketers

There are specific responsibilities that digital marketers must take on, namely:

- **Data consent rules:** Data consent refers to collecting personal data about leads and prospects via your organisation's various digital marketing channels, and gaining their explicit and unambiguous consent to opt-in to hearing from your organisation.
- **Data processing rules:** Data processing refers to how your organisation uses that collected data, and whether the leads, prospects and customers understand why it needs to be processed that way.
- **Data retention rules:** Data retention refers to how long your organisation retains personal data, and the business reasons for doing so.
- **Data transfer rules:** Data transfer refers to the transfer of the personal data of European Union citizens outside of the EU for legitimate business purposes.
- **Data deletion rules:** Data deletion refers to when and how personal data is permanently removed from your organisation's systems.

Role of the Marketing department in GDPR compliance

The Marketing department – and, by default, the head of Marketing – plays a key role in enabling, supporting, and communicating GDPR and its impact on the business to the senior management.

Because of Marketing's unique role in collecting, processing, retaining, transferring, and deleting data belonging to the public and to the organisations' users and customers, the person or people within the team nominated to roll out GDPR compliance must be fully aware of the scope and responsibilities of the project.

It is a cross-functional team effort, as the digital marketer at the head of the GDPR effort will need to work with IT, Sales, Support, Engineering, Customer Success, and Product to ensure that data privacy processes with dependencies are understood and supported across the organisation.

Data Protection Officer

The DPO (Data Protection Officer), should your organisation need to appoint one, will help steer the resources into place for GDPR compliance:

> *[The] GDPR calls for the mandatory appointment of a DPO for any organisation that processes or stores large amounts of personal data, whether for employees, individuals outside the organisation, or both. DPOs must be "appointed for all public authorities, and where the core activities of the controller or the processor involve 'regular and systematic monitoring of data subjects on a large scale' or where the entity conducts large-scale processing of 'special categories of personal data,'" like that which details race or ethnicity or religious beliefs.*

Data Controller and Data Processor

Other key terms to understand at this juncture are Data Controller and Data Processor. The digital marketer must understand in which scenarios they are the Data Controller or the Data Processor. We will dig into this more later when we talk about digital marketing channels and compliance.

The Data Controller has much more responsibility than the Data Processor:

> *The data controller is the person or body who determines the purposes and means of processing personal data. In plain English, you decide what the data is for – and what's going to happen to it... But a "processor" has a very distinct meaning under the GDPR. This refers to*

a person or body who is separate from the data controller (i.e. not an employee) and who processes personal data on behalf of that data controller. In other words, the controller gives the processor a specific job to do – and the processor does it.

It is important to know when you play either or both of these roles every time you deal with data in your job.

Legitimate business interest

"Legitimate business interest" means that there must be a clear reason for the business to collect and process particular data about a data subject (for example, a name and home address for a pizza delivery). Just because the person ordered a pizza does not mean you can then use their information to send fliers, or give their information to anyone else.

The reasons for collecting and processing must not violate any rights of the natural person. As a digital marketer, you must carefully consider: What are we collecting, and why?

That's why recording consent is such an important part of the GDPR. The consent must be freely given, unambiguous and clear to the data subject. There must not be long reams of legalese for them to read through and become baffled. Consent must be correctly recorded, and the route to unsubscribe must be just as simple and clear for the data subject.

Sensitive data

This brings us on to considering which digital marketers have the trickiest industries to deal with. If you are in healthcare, finance, public service, or if your organisation deals with natural person's data under 16 years of age, the most stringent data privacy and data protection policies are recommended. This type of Personally Identifiable Information (PII) is what is most vulnerable and requires your full attention to detail regarding GDPR.

KEY CONCEPTS OF GDPR

Introduction

Next, we are going to learn about the key concepts of the GDPR. We will aim to understand more of the key terms and understand how GDPR will change your organisation overall – in both positive and negative ways.

Key terminology

We have already touched on a few of the key terminologies of GDPR (data controller, data processor, DPO, and legitimate business interest).

Let's go through some more of the specific terminology related to GDPR:

- **Natural person:** The *natural person* is equal to the *data subject*. A natural person is an individual who can be identified based off of personally identifiable information (PII).
- **Personally identifiable information (PII):** This is any data point or combination of data points that can result in the affirmative identification of an individual person.
- **Anonymizing data:** This means there is no way to unscramble the data to link it to a data subject.

- **Pseudonymization:** This means that data is scrambled but that a key exists to decode the data.
- **Data breach:** This means that personal data has been accessed by unauthorized third parties.

Data privacy vs. data security

The difference between "data privacy" and "data security" is that:

> *Data security focuses on protecting the data from theft and breaches. Whereas privacy governs how data is being collected, shared and used.* [Varonis]

GDPR in practice

What does GDPR mean in practice for your organisation or business? For most, it means fundamental changes in core business behaviours and processes in order to incorporate "privacy by design." This means incorporating data privacy and security as standard into all of an organisation's operations – from HR to IT to Marketing.

It also means that organisations have to invest in training resources for all their employees on a regular basis. Depending on the sensitivity of the data that your organisation gathers, processes, and stores, significant resources such as hiring data management specialists and legal advisors may also be necessary.

It is important that the senior management understand what level of commitment enforcing GDPR within the organisation will take, and the cost of doing so. For the marketing team, it is particularly important as that is where public and customer data is managed.

Commercial reasons behind GDPR

GDPR is far from all bad for organisations. In fact, because GDPR shines such a strong light on data practices in organisations, the real and tangible business benefit is not only improved brand trust but also better CRM data quality.

Brand trust

There is much to be gained from promoting your organisation's level of compliance. Data privacy is of increasing concern amongst the public and your customers, and so enacting privacy by design principles will only serve to improve your brand.

Improved CRMs

Also, CRMs will become much more valuable to businesses. There is very little value in an unengaged database. In fact, the larger your database, the more your CRM provider typically charges. Why should you pay to host the data of hundreds or thousands of uninterested individuals? Having a highly engaged database means you have a subscriber list of genuine brand evangelists and hot prospects.

Data security challenges

Now, whilst there are clear benefits to the GDPR, there are also challenges. You will need to understand how your marketing data is captured from all its various sources, and subsequently, how it is stored and who has access to it.

This could be as obvious as recognising that if employees in your organisation are using personal mobile devices to access sensitive information can you guarantee that the data is safe? This is a company-wide issue, not just a marketing issue. But marketing's unique role with data puts it front and centre of GDPR.

Data breach threats to PII

The future of the digital marketer is certainly one where being a data management expert is a huge advantage. There are multiple ways that your organisation's data is at risk, and knowing how to recognise risks, set up mitigations, and respond to a data breach are becoming part of your everyday world.

There are a number of ways that Personally Identifiable Information (PII) is at risk in the Marketing department:

- **Hacks on your business database:** These occur when data is either hacked by an external entity, or when someone within the organisation accesses data that they shouldn't.
- **Leaks:** These occur when someone within the organisation with approved access uses the data through error for a purpose that the data subject did not give consent to.
- **Data becoming outdated:** PII changes over time – for example, contact details, addresses, roles for individuals
- **Data becoming unmanageable:** Data can grow to become complex and unmanageable, especially when multiple records are linked to one another

Some examples of what is considered PII are:

- Name
- Phone Number
- Home Address
- Email Address
- IP Address
- Online Profiles
- Government & Other ref numbers, Tax ID, Driver's License etc.

Responsibilities of Marketing Department

So what does the digital marketer need to maintain regularly and be rigorous about for GDPR?

1. Defining and recording email opt-ins and opt-outs
    a. design an opt-in and opt-out flow that is clear where consent can be interpreted unambiguously; ensure that opting out is as easy and clear as opting in
2. Standardizing how a new contact comes into the CRM via all marketing channels
    a. understand every data intake process of the CRM under the jurisdiction of the marketing team, and ensure that in the case of EU citizens each process has clear guidelines around consent

3. Outlining the process honouring data subject requests and deletions
    a. do a trial run of a data subject request and a data deletion request; refine and document the process, and train the relevant team members
4. Communicating data breaches
    a. understand the time frame within which you have to publish notice about a data breach, and have pre-approved comms templates at hand for a crisis scenario
5. Keeping website Privacy Page and Terms & Conditions Page up to date
    a. at regular intervals, have your DPO, IT team and a legal expert review your public-facing data usage documentation
6. Vetting and approving how CRM data is used for marketing purposes internally and externally
    a. ensure that your team members have appropriate permissions for data access within the tools they use, and that they're aware of what the data they have access to can and cannot be used for in marketing. Have an established policy regarding co-marketing or partner marketing, where the data subject is protected in accordance with GDPR regulation.

Key roles

Let's take this opportunity to review the key roles you need to be familiar with:

- **Personal data:** This means any information relating to an identified or identifiable natural person (or *data subject*).
- **Data subject:** This is an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Data controller:** This is the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **Data processor:** This is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
- **Data Protection Officer:** Duties of the Data Protection Officer include: acting on the compliance to all relevant data protection regulations, monitoring specific processes, such as data protection impact assessments, employee awareness and training employees, as well as collaboration with authorities. Therefore, the operating Data Protection Officer must not be recalled or disadvantaged due to his fulfilment of his tasks. [https://gdpr-info.eu/issues/data-protection-officer/]

GDRP and the UK

It's important to note that following the UK referendum on membership of the EU, while the detailed future for the UK may be different, the underlying policy has not changed all that much and *the GDPR is still relevant* for many organisations in the UK – especially those operating internationally.

GDPR COMPLIANT BUSINESSES

Penalties for non-compliance

Complying with the GDPR is not just an exercise in ticking a box. There are real and hard consequences to being found uncompliant. These vary to different degrees. Is your business able to withstand them?

The highest-level penalty for an organisation found to be in violation of the GDPR is a €20 million fine, or 4% of annual turnover – whichever is higher. That's the maximum. Depending on the severity of the violation, a varying degree of fine will apply. They are enforceable by the supervisory authority in each EU member state. This means that enforcement will not be the same in each country, making it hard to determine how violations will be interpreted and penalized across the board.

Loss of brand reputation

Penalties aside, there is a longer-term impact to consider: loss of brand reputation.

In a world where consumers are becoming more conscious about and uncomfortable with how much of their data is harvested and used, mostly without their true understanding, maintaining trust is critical. Trust takes a long time to build up. Word of mouth is still the most powerful marketing channel. Depending on what your organisation does, loss of trust could be irreparable and sink the organisation (for example Cambridge Analytica) or take years to recoup. Acquiring a customer is costly; preventing customer churn is one of the best metrics for organisations to increase LTV (lifetime value).

Reporting data breaches

Depending on your country's supervisory authority, you may need to report a data breach (to them) within 24, 48 or 72 hours. Your data breach preparations should involve a call to the relevant local authority within the right timeframe. In the context of GDPR, a data breach is more than personal data being stolen:

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. [ICO UK]

Part of your GDPR preparation will be to have a process in place to deal with breaches such as this, including how to communicate to those data subjects directly affected.

GDPR COMPLIANT VENDORS

Partners and vendors

It is also important to make sure the partners and vendors you work with are GDPR compliant. That includes media partners, marketing agencies and vendors within your marketing channels.

They too need to be compliant in how they handle and collect PII from your customers – this is particularly relevant to:

- Website analytics providers
- Affiliate networks
- Programmatic display
- CRM providers
- Marketing automation solutions
- Email service providers
- Remarketing services
- Lead capture providers

It is good practice to scrutinize the GDPR process and compliance framework for all vendors you work with.

SUMMARY

The GDPR strengthens data protection for all data subjects in the European Union and it contains specific guidelines covering the collection, processing, retention, transfer and deletion of data that you need to be aware of.

There are key terms to be aware of – like the difference between data protection and e-privacy. The GDPR is designed to protect personal data while the ePrivacy regulation protects an individual person's privacy in online interactions. There are also areas that are particularly sensitive like financial, health and underage data.

There are also valid commercial reasons behind GDPR – like protecting Trust with customers and maintaining 'clean' data within your business but there are many threats presented by personal data like data leaks, data becoming outdated or unmanageable, being hacked or misused by others.

The Marketing department and Head of Marketing play a key role within the business in being GDPR compliant including responsibilities for: opt-ins, new contacts, processes covering data subject rights, communicating breaches, website terms and vetting CRM data to be used by partners for marketing.

There are specific roles to be aware of covered by the GDPR like: Data Controllers, Subjects, Processors, Data Protection Officers and Supervisory Authorities.

Finally, if that's not enough there are direct penalties for non-compliance like fines and reprimands also potentially a right to compensation, as well as indirect damage to be aware of like loss of trust, reputation damage and a potential loss of ability to grow partnerships.

NOTES

LESSON 2: PREPARING YOUR BUSINESS FOR GDPR

EXISTING DATA PROTECTION LEGISLATION

Introduction

Now that we've a clear picture of the scope of GDPR, you'll appreciate how important it is to any company and organisation doing business in the European Union.

To be successful, it's important that there's 'buy-in' throughout a company and organisation in meeting these higher standards – both off-line and on-line.

In this next section, we'll also look at how some brand owners have gone above and beyond to build a much deeper level of trust with customers, clients, supporters and employees.

It's about understanding how to implement transparency, accountability and give control to the individual over their personal data – not just from a marketing perspective but wherever their personal data is being processed.

We'll then move on to discuss how to prepare marketing in the world's biggest digital single market of 500m consumers.

We'll consider the previous legislation around this and how the GDPR is an evolution in data protection regulation on a global basis.

We'll also provide some insight to the requisite level of knowledge, skills and experience that individual digital marketers need to possess at various levels within the marketing department.

At the end of this section, we'll focus on things senior digital marketers must have on their 'to do' list.

This includes reviewing roles and responsibilities within the marketing department, working with colleagues from HR.

It includes reviewing contracts with third parties that may be processing personal data on our behalf, ensuring sufficient safeguards and guarantees are in place.

And it includes making sure that tools used don't increase the risk of harm or damage when processing personal data.

General data protection regulation

The GDPR is not a totally new concept for digital marketers. There have been laws governing data in place for years. Not all have had the publicity behind them that GDPR has, but they have been in place. The extent to which digital marketers have been aware and actively considering compliance varies significantly across the industry.

Regulations vs. directives

The GDPR is different to the existing European Union legislation in a key area – it is a regulation, *not* a directive. What does this difference in semantics mean? It is important for digital marketers (who need to become more fluent in legalese) to know the difference!

Regulations

A regulation is a binding legislative act. It must be applied in its entirety across the EU. For example, when the EU wanted to make sure that there are *common safeguards on goods imported from outside the EU*, the Council adopted a regulation.

Directives

A directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. One example is the *EU consumer rights directive*, which strengthens rights for consumers across the EU, for example by eliminating hidden charges and costs on the internet, and extending the period under which consumers can withdraw from a sales contract.

DATA MANAGEMENT EXPERTISE

Training

As digital marketers, we know that the future of the profession involves more data, not less. When we think about the current state of marketing automation and marketing analytics, and the new future of artificial intelligence and the internet of things, it is inevitable that our knowledge and understanding of data management and data laws moves in lockstep.

As such, regular data management training of digital marketing managers up to CMO level will become part and parcel of the role. There are a plethora of expert consultants out there, and law firms, that have specialised in GDPR and data privacy and security as a whole. Working with advisors that are deeply familiar with the European Union's legal framework is essential. Your organisation's commitment to being compliant will provide a sound case for any audit that may occur down the line with your country's data protection commissioner or department.

GDPR knowledge requirement and marketing roles

Middle and upper marketing management will need to know the complete workings and impact of GDPR on the marketing team as a whole. But what about individual contributors? Let's look at the example of an average digital marketing team, built around the content marketing model, as a case in point.

Development

- Website forms are set up correctly
- Website plugins are compliant
- Website platform is secure
- CMS is integrated correctly

Data analysis

- Analysis tools are compliant
- Integrations are used where possible to prevent exporting data onto computers

Graphic design

- Internal-only company information is not used on public-facing graphics

- Customer data used for public-facing content must have signed and recorded explicit consent

Copywriting

- Internal-only company information is not used on public-facing content
- Customer data used for public-facing content must have signed and recorded explicit consent
- Contractors must not have unauthorized access to CMS data

Product marketing

- Must help ensure privacy by design is the standard for products, where applicable

PR

- Gain, record and maintain consent from media contacts to send materials
- Prepare data breach communications
- Maintain a trustworthy brand regarding data management

Events

- Gain, record, and maintain consent from booth visitors before adding them to your CRM for marketing
- Check the event attendee list terms and conditions (Are the attendees aware that they signed up to receive communications from your organisation, and what communications align with those expectations?)
- Review the policies of any third-party apps and services you use to run or attend an event (Who owns the data, and is it secure?)

Digital marketing

- Privacy impact assessments (PIA) on all processes and projects

GDPR Resources

There is quite a bit of confusion out there on what GDPR is and isn't. And whilst a legal counsel is your safest bet, it is good to know where you can go for accurate information and updates.

- **The EU GDPR Portal:** (https://www.eugdpr.org/) This is run by the European Union itself.
- **The GDPR Awareness Coalition:** (http://gdprcoalition.ie/) This is an Irish non-profit organisation that came together to assist all business prepare for the regulation.
- **Council of Europe Data Protection: (**https://www.coe.int/en/web/data-protection/home) You can also find your local country's data commissioner office a useful source of information.
- **Smart Insights:** (https://www.smartinsights.com/tag/gdpr/) This gives specific advice for marketers, and is UK based, so they will have Brexit in mind when posting their informative content.
- **Forrester's GDPR articles:** (https://www.forrester.com/search?tmtxt=gdpr&searchOption=0&source=typed#) This is full

of useful observations, summaries, and insights for B2B, B2C, marketing tactics and industries.

Always check the quality of your sources! If you are using any of the publicly available advice in your day-to-day business, ensure that your DPO or the Data Commissioner or your legal counsel approves.

Data protection by design and by default

The GDPR should become part of your "business as usual" in marketing. It should be as standard as checking your Google Analytics data.

Data privacy by design is a proactive, risk-minimizing approach to digital marketing that enhances rather than hinders your marketing. As Econsultancy summarises:

> *"In short, the GDPR requires:*
>
> - ***Data protection by design:*** *Data controllers must put technical and organisational measures such as pseudonymisation in place – to minimise personal data processing.*
> - ***Data protection by default:*** *Data controllers must only process data that are necessary, to an extent that is necessary, and must only store data as long as necessary."*

Later, we will dive into the practicalities of privacy by design, and privacy impact assessments (PIAs). For now, just understand that digital marketers should actively educate themselves on data legislation and what it means for their day-to-day activities and strategies.

BUYING IN TO BEING GDPR COMPLIANT

GDPR accountability

It is important to understand that GDPR is not simply an IT team responsibility, or a HR department one. GDPR is a sweeping, all-encompassing regulation for organisations. Organisations need to comply with internal data held on their own employees, as well as comply with data gathered from externals.

Apart from appointing a DPO, your organisation (depending on its size) needs a representative from each department to form a cross-functional task force. The project manager of this task force needs to assess the GDPR requirements for each department, and put in place a plan where the dependencies are made transparent. For example, there isn't much use in the marketing team putting a data deletion process in place if the data subject's data exists in another department's system as well.

The consequences for the organisation, as well for the individual, should be made clear to all on the task force by the DPO. A company-wide education session would also be an excellent idea.

Levels of compliance for an organisation

As mentioned previously, your organisation's industry will determine the level of buy-in for data compliance. It is especially important if you work in finance or health, or deal with underage data. This is not to say that other industries or types of organisations should not take the GDPR seriously; but it does mean that particular diligence is required in those areas as the data is extremely sensitive.

As well as that, the GDPR states the following as sensitive data in Article 9:

> *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

Organisation-wide alignment is the only way to ensure GDPR compliance for the marketing team.

THE MARKETING FUNCTION

Team members' roles and responsibilities

Now that we have covered GDPR at the company level, it is time to cover GDPR at the marketing team level. Marketing has a particularly important role to play in GDPR. Because of the amount of data collection, data processing being undertaken on a daily basis, as well as email marketing, care must be taken to be fully compliant.

To understand what each team member needs to know in order to do their job correctly, start with their contract. What are they officially responsible for? Are there areas of responsibility without a clear owner in the team? Ensure that all marketing activities have an owner, and then you can understand who does what in terms of GDPR compliance.

Roles requiring GDPR education

GDPR provides a good opportunity to perform a training needs analysis (TNA) on the team in terms of preparing for a future of formalised data privacy. You should work with your head of marketing and HR to assess what roles require education to bring them up to speed. With GDPR, guesswork is risky. By performing a TNA you are mitigating that risk.

External contracts

Once you have an understanding of the responsibilities internally in marketing, you can then turn towards external contracts. Marketing teams frequently work with event vendors, contractors and agencies. Your team must document all of these in a single place, as this will make the auditing (and management) process far easier.

Mark those on the list that involve the exchange or processing of data. Identify which of this subset involve sensitive and personal data. Next, understand which of these relationships cannot continue due to GDPR non-compliance (in particular, any vendors that are US based, as the US has relatively low data compliance). For those that remain on the list, identify the risks and mitigations that can be put in place. For example, for an agency that has access to your marketing automation software, you can change their permissions to access, import and export data.

Understand who on the marketing team owns each relationship.

Assessing marketing tools

Next, you need to perform a similar audit of the software and tools each team member is using to perform their role. This gets as granular as browser plugins, website plugins, popup tools and badge scanners at events.

As with the audit of your contractors, list the tools, and assess which ones process personal data and sensitive data. Each tool will have Terms and Conditions that need to be reviewed, as well as their privacy policies and data security policies.

Anything that fails GDPR compliance cannot be used going forward.

For those that pass, as before, list risks and mitigations.

Events and website

Of particular interest to the digital marketer will be events and the website.

Events

How do you currently spread awareness of an event your organisation is hosting or sponsoring? What channels and tactics do you use? If your goal is lead generation, how do you do that? If your goal is brand awareness, how do you measure that? At a customer event, are you prepared to answer all of their GDPR questions? Basically – do your event goals – and subsequent ROI reports - involve the gathering or processing of personal data?

Whoever is responsible for events needs to perform an audit similar to the overall team audit, as event management is complex.

Website

For those with inbound marketing strategies, each method of data intake and processing needs to be understood and made compliant. This includes popups, forms, cookies and tracking software. Each tool used for this needs to be vetted for compliance. Are you the data controller, and are they the data processor, at all times? Do they keep a copy of the data? Have they got access to your organisation's systems that contain personal data?

Again, as with events, the website is a project in its own right, and requires vigilance in terms of compliance.

Anonymisation vs. pseudonymisation

As you and your department prepare for GDPR, you will need to know where data obfuscation techniques can be best used. The two options available are anonymisation and pseudonymisation. You can consult with IT on how to apply either technique.

Anonymisation

Anonymisation means to completely render the data unidentifiable. That is, no matter what pairings of data are made, the data subject can never be identified. For example, having someone's job title and company name can often lead to directly identifying them. Anonymisation prevents this from happening.

Pseudonymisation

Pseudonymisation is much more limited. This means replacing data points with a key, obscuring but not eliminating the data subject from being identified. The person able to uncode the pseudonym

remains the data risk in this scenario. For example, using serial numbers instead of names on blood samples is pseudonimisation.

SUMMARY

There have been data privacy and security standards which marketers have had to adhere to for many years, but GDPR is different in that it is a regulation which will be enforced whereas the previous Directive served more as a guideline for best practice. However, GDPR is not the only data compliance legislation that may impact your business. It's important to know about any legislation within your target market which may affect you.

The goal is to build compliance into all marketing processes and projects as standard – so that you make 'data privacy by default' and 'privacy by design' the standard.

While some organisations will require higher levels of compliance, there must be buy-in across the business with all departments aligned to become GDPR compliant.

In order to review the Marketing function for compliance, you can start with HR to understand roles and responsibilities of team members. It's also important to review contracts with external partners and agencies – documenting a risk assessment for each. You can assess the tools that team members use for compliance and document a risk assessment for each.

Finally, look at the processes for data intake, processing, transfer and security with regard to events and the website, assess for compliance with GDPR and document a risk assessment.

NOTES

LESSON 3: DATA PROTECTION IMPACT ASSESSMENT

ROLE OF DPIA IN GDPR

Introduction

So how do you begin to understand what's required of the marketing team for compliance with the GDPR?

The solution is to use a project management approach where you'll have the broad focus areas mapped out and the dependencies aligned.

The next step is the nitty-gritty, "what actually needs to get done?"

In this section, we'll go over what you need to do to run a Data Protection Impact Assessment or DPIA for short.

We'll talk about the circumstances in which an assessment is required and also importantly when you might want to carry out a DPIA in a non-mandatory situation.

It's also important to consider the key individuals you'll work with internally in your company and organisation to conduct a DPIA, what information they require from you and the information they'll require from the wider marketing department.

We'll discuss the key elements that go into a successful DPIA and each of the steps you must go through when carrying out a successful DPIA.

Finally, we'll summarise why it's important to make sure future projects and systems are compliant with the core principle of data protection by design.

Data Protection Impact Assessment (DPIA)

A DPIA is an audit done on existing processes and projects that involve data in the team, and on imminent processes and projects (the world doesn't stand still for GDPR!). This means assessing a process or project for personal and sensitive data risks, assigning a level of importance and likelihood of occurrence, and then designing an appropriate mitigation for each individual risk.

Conducting a DPIA

A DPIA is to be conducted by the GDPR subject matter expert where the following is involved:

- Evaluation of a data subject based on sensitive or personal data
- Automated data processes that result in discrimination
- The processing of a data subject's data where they are unaware of your use of it
- Processing large quantities of data
- Processing data from a middleman service
- Processing data of the vulnerable or underage
- Assessing a new process of taking in data
- Transferring data outside of the EU
- When the processing of the data in itself "prevents data subjects from exercising a right or using a service or contract"

Keep the documentation of your DPIAs for future auditing purposes. Based on what you discover during these DPIAs, they will inform your GDPR project plan. You will better understand what is most urgent and what your final GDPR goals for marketing will look like in practice.

GDPR and DPIA

As you can guess from the description, these DPIAs are not once-off. You and your team (and all digital marketers) will be performing DPIAs repeatedly. This is great for continued compliance with GDPR, as the digital marketing landscape is always changing. DPIAs will ensure your organisation is at minimal risk, and builds in "privacy by design."

Does this mean you only apply DPIAs to the scenarios listed above? Apply it to all your team's activities with data. Not only will it embed a necessary habit, but you'll be able to push your brand even stronger with its data privacy message. It will boost your customer referral and evangelist programs as well as simply being the right thing to do for the people whose data you have been entrusted with.

REQUIREMENT OF DPIA IN MARKETING

Key stages in DPIA

Let's look in more detail at what is meant by performing a DPIA on a marketing team process that involves personal, sensitive, or third-party data processing. You may need to go outside of marketing to follow the journey of the data from end to end.

If we to walk you through the process of a DPIA on importing leads gathered from an event. Ideally, you will carry out future DPIAs in advance of the data processing occurring – but for now, let's look at this through the lens of it being the first time.

- **Identify the need for a DPIA:** We are in possession of people's personal information – names, addresses, companies they work for, job titles, phone numbers and email addresses.
- **Describe the information flow:** Anonymous individuals arrive at our booth at an event; they speak with members of the organisation; they hand over business cards or they have their event badges scanned by a team member; the business cards are collected by the event manager and the scanned badges list is acquired from the event organizers; the event manager compiles all the data into a single spreadsheet and cleans it; the data is imported to the CRM and mapped; the data subjects become leads and are assigned to sales team members for nurturing; the event manager analyses the data subjects' progress through the sales cycle in order to create periodic reports on ROI
- **Identify risks:** Handing over a business card or getting a badge scanned is not explicit recorded consent to receive communications from your organisation; the event organizer has a copy of the data – are they the controller or the processor, or are you?; mistakes are made compiling the spreadsheet of data; mistakes are made importing the data; unauthorized team members at the event may access the data subject's information; the sales team may not actively seek out consent when performing their initial outreach; the event manager may not pseudonymize the personal data for their reporting purposes; the data may not get deleted once it legitimate business interest has expired
- **Identify mitigations:** Ask for consent directly at the booth and record it through your own digital system (for example, with an iPad and a landing page); get information on the event's GDPR compliance in advance and understand data roles; have a second team member review your spreadsheet for errors; ensure that the team CRM expert imports your data; train

the sales team to ask for or reconfirm consent for communications – ensure they can record it for auditing purposes; the event manager gets support from IT on pseudonimising personal data so that reports can be run without compromising the data subject over and over; work with IT, sales and marketing to develop a rolling data deletion process

- **Get your DPO to approve the new process**
- **Integrate into your next event**

As you can see, a risky process such as importing event leads now involves low risk. It involved sales, marketing, and IT as well as signoff from the DPO.

Publishing a DPIA

Do not assume that DPIA documents are always going to be private, internal documentation. There are scenarios in which your organisation are compelled to or may volunteer to publish a DPIA.

> *It is not legally mandatory to publish the DPIA. However, there are a number of benefits to doing so. Publishing the DPIA can help to foster trust in your handling of personal data, and demonstrate accountability and transparency, particularly where members of the public are affected. This may be especially beneficial for DPIAs carried out by public bodies.*
>
> [DPC Ireland]

If your DPIA results in a high-risk scenario that you are uncertain of being able to mitigate, you should consult with your country's data protection commissioner.

THE DPIA PROCESS

Introduction

A DPIA is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is required at least in the following cases:

- A systematic and extensive evaluation of the personal aspects of an individual, including profiling
- Processing of sensitive data on a large scale
- Systematic monitoring of public areas on a large scale

As such, having a process in place to carry out a DPIA correctly will be hugely valuable to you, your team and your organisation.

Key elements of a successful DPIA

First, establish who carries out DPIAs in which scenarios. Will you centralise it to one team member, or make it part of your individual contributors' day to day work? Who will collate, document and safeguard the DPIAs once complete? Who will communicate the DPIAs to the DPC that are necessary, or would benefit from doing so? Your first step is appointing those responsible and ensuring they have complete understanding on what they need to do. Keep your DPO in the loop – they may have useful suggestions.

A high-level explanation of a DPIA goes as follows:

- Document why a process is relevant for a DPIA
- Identify the process under scrutiny, and note whether it is a process improvement or a new process
- Acknowledge that improving an existing process means there may be legacy data to deal with as well as new data post-implementation
- Evaluate the cost of performing the DPIA – how many hours of whose time will be required to complete it
- Evaluate the value gained by completing the DPIA
- Identify the risks to the data subjects
- Identify the mitigations to these risks
- Document and decide if it needs to be made formally public, and if so, to what degree

Steps involved in carrying out a DPIA

When you are trying to pin down what a "process" is, focus on what is important in the GDPR – the active consensual acquisition, use, storage and deletion of personal data. Once you have an audit done on how your team deals with each of these stages, you can tease out the details on how data is managed in marketing campaigns, the CRM, in advertising and so on.

Prioritise processes with the highest risk, and their dependency processes.

Using your project management tools and methods as a framework, begin mapping the following per DPIA:

- **Assess whether you need a DPIA:** Consider the reasons why you consider the data touched by your process to be subject to a DPIA. (For example, I am running a children's art workshop, so I am potentially dealing with data under the digital age of consent, as well as health data. I am using an online events platform for registrants so I do not know if my setup is safe.)
- **Describe the information flow:** What are the steps to achieve the outcome? (Take the example of an art school. The parent finds an advertisement on social media >> they click on the link to the events platform >> they submit the details of their child on the form >> a security email is triggered to ensure the email account is verified >> the registration is confirmed on email double opt-in >> attendance is confirmed on receipt of payment >> payment occurs via online transfer >> the parent and child's information is stored in the CRM until the day of the workshop >> unless the parent has opted in to hearing from the organisation in the future, the data of both parent and child is deleted from the CRM and the event platform.)
- **Identify risks:** Identify the risks at each stage of that data journey. (For example, which of these tools are data controllers or data processors? How do I ensure these tools do not have unauthorised access to my CRM? How do I ensure the parent and child are who they say they are? How do I record consent to email? How do I delete the data at the end?)
- **Identify mitigations:** Identify the mitigations for each stage. (For example, not allowing third party access to the data, not keeping the data beyond the day it is needed, using secure and compliant vetted tools for events, payments and CRM, not allowing others unauthorized access or use of the data, ensuring knowledge of the tools so no accidental data manipulations or deletions occur)
- **Assess risks:** Assess if all risks can be mitigated. If not, why? Should your organisation take on that risk?
- **Get approval:** Discuss with the stakeholders of the process and agree on how to proceed.
- **Document decisions:** Document everything.

DESIGN COMPLIANT PROJECTS AND SYSTEMS

Privacy by design

As you work through your existing processes, and bring them up to the required level of compliance, you will refine the best process for your team and your organisation in how to incorporate "privacy by design." Building good data privacy habits into organisations is what the GDPR is all about.

We've talked at length at the brand value, and therefore financial value, of being compliant. Whilst that is the carrot, avoiding prosecution and heavy fines is the stick. Marketing teams grow, have turnover and iterate fast. By having privacy by design built in to how you do work from day 1 means that maintaining data privacy excellence, and therefore ensuring compliance, will not be perceived as an additional burden. It will be business as it should be.

End-to-end compliance

By carefully auditing your digital marketing processes, you will discover that you are not only responsible for compliance at the beginning of the sales and marketing funnel, but all the way through it. Take particular care with your customer's data and any referral programs you have in place. Customer retention is far more profitable than having churned customers. Delighting your customers in return provides a steady flow of future business, when referrals are done right. It is a mutually beneficial relationship.

Be transparent with them on your data privacy. Send communications about it. Deliver trustworthiness.

SUMMARY

A Data Protection Impact Assessment is an audit of either an existing or incoming processes, projects or changes in the company whereby the data risks are assessed and documented, and risks recognized and mitigated where possible.

And when is a DPIA required? Well, if a processing activity is likely to result in a high risk to the rights of natural persons then it's the responsibility of the controller to carry out an impact assessment. Sometimes it's also a good idea to carry out a DPIA in a non-mandatory situation – for one thing it shows the organisation's commitment to data best practices and also increases trust and therefore improves brand power.

To carry out a DPIA, you first need to recognize who to work with internally to conduct the audit - - for example, Sales, IT, Customer Support – you also need to understand the information you require from them and what information they will require from marketing also.

The elements of a successful Audit involve a description of the new process incorporating the data management requirements, an assessment of the value of the new process versus the purpose, the risks to the rights and freedoms of data subjects and the mitigations that can be put in place to safeguard their rights and freedoms.

So what are the steps you should take when carrying out a DPIA: First, it's important to explain why the Audit is required, to describe the data flows from end to end and to document the risks and describe how they relate to the rights and freedoms of data subjects. You also need to document

the solutions to the risks and get agreement from all stakeholders on the assessment and where appropriate to get input from data subjects.

Finally, it's important to understand that the digital marketing experience must be compliant from end-to-end of the customer journey. The value of keeping data compliance front and centre of each project is brand value and therefore is ultimately critical for your business.

NOTES

LESSON 4: ONGOING GDPR COMPLIANCE

COMPLIANCE ACROSS DIGITAL MARKETING

Introduction

In this final section, we'll look at personal data processing likely to be undertaken by digital marketers as well as consider new reporting and logging requirements under the GDPR.

We start by examining the data intake process and how personal data is gathered and logged in accordance with the GDPR. This covers website forms, content syndication, social media lead generation, trade shows, co-marketing and referrals and affiliate marketing.

We'll then go onto discuss how to comply with the higher standards around processing and security by implementing appropriate organisational and technical measures.

In this section, we'll also look at the transfer of personal data and where processing is done outside of the EU as well as how to effectively handle subject access requests from customers and clients should you receive them.

We conclude by discussing how best to assess, practise and document personal data deletion and rectification requests as well as the importance of handling a personal data breach – how it's communicated to stakeholders and authorities and when personal data disclosure is permitted.

Data intake points

Let's flush out all possible data intake points that you need to audit:

- Website cookies
- Tracking pixels
- Website forms that collect Personally Identifiable Information (PII)
- Content syndication
- Social media lead generation forms
- Sponsored trade shows and events
- Internal events
- Co-marketing and partner marketing
- Referrals
- Business connections

Ensure that your audits and ensuing DPIAs have bottomed out every risk involved to personal data via these tactics. Ensure that your CRM is set up to support your newly improved data intake processes. Take care to manage legacy data differently to new data, if you make fundamental changes to any of those listed above.

Remember, your company can be liable if there is a PII data breach in the marketing channels in which you operate – for example Facebook, Google, and so on.

Data privacy processes

Data privacy as a process in itself needs to be regularly reviewed and trained on. What works today may not work in the future. Local laws may supercede EU laws. Amendments may come into play. The law is ever-changing, and so, you must adapt to remain compliant.

The documentation of your data privacy process is exceptionally important in the instance of an audit, whether your organisation deals in highly sensitive personal data or not. Your organisation is accountable to the data subjects of the European Union – simple as that.

Data security processes

We've seen that data security and data privacy are not the same thing. However, it would be remiss not to make at least a short reference to security. All the privacy in the world is of very little value if your data is not secured from malicious access. Be generally aware of your organisation's level of data security so that you can correctly presume the risks to data privacy in your DPIAs. Your IT team and DPO will be glad to help you understand how it works, if it is unfamiliar.

Data transfer processes

You need to be aware when data is being transferred internationally, and why. There must be certain administrative steps taken in advance of a data transfer. Ensure to have a process documented on how to do a data transfer correctly, and a clear person assigned to carry out the marketing team's part in it.

Subject access request processes

Be aware that in the case of a data request – whereby a data subject has requested a copy of all the data your organisation holds on them – that marketing's data is most likely where it begins, but not necessarily where it ends. During your audits and DPIAs of existing and future processes, you will uncover how personal data moves from marketing to sales, IT, HR and perhaps other internal systems and tools. It is your responsibility to provide the marketing data; but you must understand that there may be traces of data elsewhere. This is where a cross-functional GDPR team is essential in order to be fully compliant.

Having a landing page where a data request can formally be made by data subjects is a great way of recording it, and honouring the 30 day turnaround limit (except in exceptional circumstances, to be agreed upon with the DPC). The data must be compiled and presented in an easy-to-read and accessible file format to the data subject by the end of the request deadline.

The data request process is extremely useful to consider when dealing with a data deletion or data correction request. Again, track down all the data within marketing systems, but also understand where it exists outside of marketing. For example – you may delete or updated a data subject's profile in HubSpot, a marketing database software, but they may still exist in Salesforce, the sales database – and therefore the data could be automatically synced back in at any time.

Data deletion process

The data deletion needs to occur in a logical order throughout systems.

A difficult question to answer with data deletion is the chicken and egg scenario: If I don't keep a copy of the data subject's email address to prove that they requested a data deletion, how can I prove it at an audit? This item is still not clear at this point. Get direction from your DPO and DPC to make the best decision for your organisation, as all organisations are different.

Data breach processes

A data breach is more than getting hacked. It is any unauthorized access, unauthorized use or unauthorised deletion or manipulation of personal data of a data subject. You have 72 hours to report the data breach to the commissioner, unless there is good reason. The GDPR states:

> *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*
>
> [source]

It is good practice to have a data incident team appointed to apply the mitigations and prepare the necessary communications to those affected. Clear roles and responsibilities in these situations are vital. Preparing in advance for highly likely data breach scenarios is extremely likely to reduce the overall cost of the breach to the organisation.

Data disclosures

If your organisation is approached and requested to disclose data subjects' private data, you should get legal counsel to determine the need. The GDPR is not entirely clear to the layman on what would constitute reasonable grounds for data disclosure. It would depend on local country laws as well as international agreements.

SUMMARY

Finally, let's review the ongoing requirements across digital marketing processes.

For data intake processes that includes looking at website forms, content syndication platforms, understanding your role as a processor or controller with social media lead generation, gathering data for tradeshows and events, understanding your role when using partner marketing, and referrals or affiliate marketing.

For Data Privacy and Security processes it involves aligning marketing processes with data privacy and security processes and documenting the risks and mitigations. For data deletion, correction or subject access request processes, assess, practise and document how these are completed within your organisation. With data disclosures, you need to understand the circumstances whereby a data disclosure is permitted.
Finally, for a data breach – assess, practise and document how it is audited, how it is communicated to relevant stakeholders and authorities how it would be resolved in your organisation.

NOTES