



ALL YOU NEED
TO KNOW ABOUT
GDPR

TABLE OF CONTENTS

Introduction	04
1. What is GDPR? What is the purpose of GDPR?	05
2. Policies and Data Subject Rights under EU GDPR	06
2.1 Increased Territorial Space	06
2.2 Penalties	07
2.3 Consent	07
2.4 Breach Notification	07
2.5 Right to Access	07
2.6 Data Erasure/Right to be forgotten	07
2.7 Data Portability	08
2.8 Privacy by design	08
2.9 DPO	08
3. Industries that will majorly get affected by EU GDPR Regulations	10
4. EU Compliance	11
4.1 Data Control	11
4.2 Data Security	11
4.3 Data Breach	11
4.4 Risk Reduction Strategy	11

TABLE OF CONTENTS

5. Steps for EU Compliance	13
5.1 Understand GDPR	13
5.2 Create a Data Map	13
5.3 Classification of Data	13
5.4 Begin Data Evaluation	13
5.5 Access Document and Risk Management	14
5.6 Revise and Repeat	14
6. Some Helpful Statistics	15
7. Effects of GDPR on Events Industry	17
8. Effects on Event-Tech Companies/vendors	19
9. Expert's Opinions	21
Resources	23
Conclusion	24
About Hubilo	

INTRODUCTION

One of the EU's biggest law that is coming into action from 25th May is all organisations and companies across the globe are worried about. Agreed, it is a revolutionary change that is impactful for all the companies in EU and those dealing with EU clients. So awareness about the same is quite essential.

In this whitepaper, we have covered all the basic knowledge one needs to know about GDPR i.e. General Data Protection Regulations. We have also covered a few basics for the implications of these regulations on Event Industry and Event Tech Providers.

WHAT IS GDPR? WHAT IS THE PURPOSE OF GDPR ?

These questions have been a hot topic of discussion for a past few weeks now. In the year of 1995, European Union adopted a directive in order to protect the privacy of their citizens and is now altering the directive's rules and regulations with the current world scenario. Hence, to solve the privacy issues, GDPR came into light.

GDPR : General Data Protection Policy is one of the major policy changes that will effectively implement from 25th May'2018.

GDPR is basically a set of rules and regulations that digitally monitors and keeps a tab on how the citizen's data is being processed and for what purposes. It is a matter of protecting personal data of people residing within EU.

GDPR creates transparency between various businesses that collect the citizen's data and the people who would like to have access to how their data is being used.

POLICIES AND DATA SUBJECT RIGHTS UNDER EU GDPR

EU General Data Protection Regulation is a massive change in the business community all around the world. What are the policies of GDPR that must be adhered to and kept a count for if your event or business involves collecting data?

2.1 Increased Territorial Space

One of the major policy changes that are coming with the data privacy regulation is that it is applicable to all the companies that can or will require data of EU's residents.

Previously, this policy wasn't made clear so people across the globe didn't take it seriously until recently. So, all the businesses must complete their paperwork in accordance with the laws and rules established.

This EU GDPR policy is also applicable to the organisations outside EU who are currently engaged with business in EU or maybe in future will have business ties in the Union.

EU businesses who tend to process data of the citizens are also supposed to have a representative to back them up to check the legitimacy of their activities.

CHAPTER 2

2.2 Penalties

If an organization is found guilty of breaching the GDPR policies then it will be liable to pay 4% of the Annual Global Turnover or €20 Million.

2.3 Consent

The conditions under this section have been legalized and a company will no longer be able to use illegitimate or unauthorized forms in any manner to collect EU citizen's data. Consent for the data must be legal, clear and written in plain language for easy understanding.

2.4 Breach notification

Under EU GDPR regulations, notification for breach will be mandated from 25th May onwards and it must be notified within 72 hours of first having become aware of it. Data Processor Officer will be in-charge of informing all the customers and controllers about the breach without any delay.

2.5 Right to Access

Under the policies laid by the EU government for GDPR, the data subjects i.e. the citizens of the Union are entitled to access the procedure of how their data is being processed and the purpose for the same.

In addition to accessing their information, the data subjects will also be provided a copy of their personal data in a digital format, free of charge.

2.6 Data Erasure/Right to be forgotten

It is one of the crucial and a fair point on the part of data subjects. Data subjects can have data controller erase all their personal data and have authorities stop any processing of their data via third parties.

CHAPTER 2

This comes into action when the processing of data becomes irrelevant to the purpose or when the data subjects withdraw their consent.

2.7 Data portability

Under the EU GDPR policies, data subjects have the right to receive their personal data in a digital format and share it with another controller.

2.8 Privacy by design

Though it has existed as a concept on paper for years, but, is now getting implemented. Privacy by design focuses on designing the systems so as the data is secured and not adding features to the existing systems to protect the data.

2.9 DPO

The introduction of a Data Protection Officer is a new addition to the GDPR regulation. DPO's position will be provided to such an individual that'll look upon that the new laid laws and practices are being followed.

DPO will have to be appointed in all the offices that in any way will do business with European Union or collect the EU citizen's data at any point of time. The following are the roles of a DPO-

- To ensure security and safety of data
- To conduct privacy assessments internally
- To report those who won't comply with the new rules

CHAPTER 2

- To monitor data activities in order to protect it and have all the necessary security and risk management aspects sorted
- Be in contact with the superiors if in any circumstance someone's data is being processed
- To manage and view all the legal documentation

All the companies on which GDPR rules are going to imply must appoint a DPO to meet the policy requirements.

INDUSTRIES THAT WILL MAJORLY GET AFFECTED BY EU GDPR REGULATIONS

Companies are bifurcated in separate categories, one is “controllers” and the other is “processors”. Companies that fall under the category of “processors” actually deal with the personal data of data subjects. For “processors” it is essential to maintain all the personal data records and how they are being processed. The companies that fall into this category are more legally liable to held responsible in case of a data breach.

The other category, “controllers” although doesn’t process the data but are obligated to follow the terms and conditions of the GDPR policy once they forward the data to the “processors”. The companies under this category must also have full compliance with GDPR.

Regardless of where the organization is physically located, if it has a web presence and offers goods and services within EU boundaries, it must follow GDPR guidelines. Significantly the industries that are going to be majorly affected by GDPR are service providers, marketing and service providers, automobile industry, finance and IT industry.

Companies based outside of EU are also headed towards a deadline for EU GDPR compliance. So, wait no more and move to the next section to know more about EU Compliance.

CHAPTER 4

EU COMPLIANCE

The main motive of the EU Government for strongly implementing GDPR is to return citizens right to their data sharing and security. Under the EU GDPR compliance, following have been mandated for the organisations:

4.1 Data Control

In order to ensure the security of the citizen's data, use it for the authorized purpose only, which in turns reduces it's exposure to the third party entities.

4.2 Data Security

Implement high data security measures to preserve the information collect- ed of the data subjects. For tech-based industries, data encryption must be a priority.

4.3 Data Breach

In case the organisation is under a threat of security breach necessary measures must be taken at the earliest i.e. authorities must be notified within 72 hours without undue delay.

4.4 Risk Reduction Strategy

Implement the compliance measures properly and ask all the third party customers to comply with it as well. There must a risk management policy prepared by all the companies in order to handle any critical situation.

CHAPTER 4

Few extra pointers to keep in mind

- Organisations complying with GDPR must only process data for authorized purposes
- Organisations and companies should make sure of data accuracy and integrity
- Update all the policy documents and legalize it
- Create awareness of the GDPR policies and distribute the notice about the changes to one and all
- Make sure to have the consent to use data in a valid form or document
- Create a database with all the entries of the data reviewed in detail
- Implement all necessary data security measures—Encryption of EU citizens data

STEPS FOR EU COMPLIANCE

It is a 6 step process for organizations to prepare for GDPR compliance -

5.1 Understand GDPR

It's not just securing data but many other regulations and data features are implicated in businesses and corporations under EU Government. The EU legislation has laid down all the rules of collecting and processing its citizen's data.

5.2 Create a data map

Research, discover and document every little detail you come across which includes all the decisions, all the acts under regulation and the risk factors related to data.

5.3 Classification of data

GDPR legislation has categorized the data (whether privacy factor applies to it or not), determine whether the data collected by your organization falls under any special category defined by GDPR. If yes, then how to access and process it further and to whom the data be shared with?

5.4 Begin data evaluation

Evaluate the data collected by setting a priority to it. Research in-depth about the private data, its review policies and procedures. Apply the required security measures to protect any data breach and secure it in the repositories once assessed.

CHAPTER 5

5.5 Access document and risk management

Have a risk management strategy for all the data that your organization has collected. Investigate the data thoroughly and made proper documents about it.

5.6 Revise and Repeat

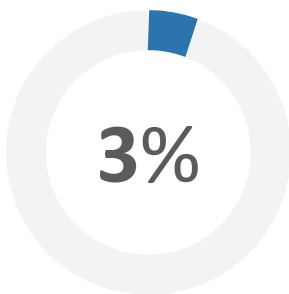
Last but not the least, repeat the above 5 steps whenever necessary.

SOME HELPFUL STATISTICS

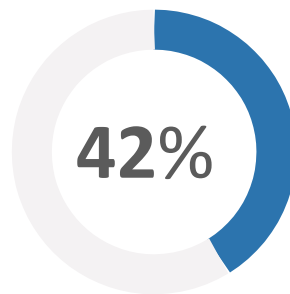
As the deadline for the GDPR enforcement is approaching, many organisations are making attempts to understand the policies and to comply with them if applicable.

But a few months before, various companies lacked the understanding of EU GDPR policies and rules. A survey was taken at that time which depicted the lack of global understanding amongst people for GDPR.

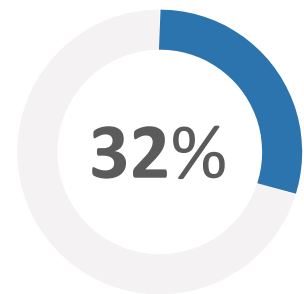
Few statistics here show the results of the universal survey:



Just 3% of professionals whose role involves consumer data collection, storage, or processing fully understand what is covered by the upcoming GDPR



Only four in every ten say their company will use independent legal advice



One-third anticipate a significant impact, despite a lack of understanding

CHAPTER 6

Another survey conducted by PwC of 200 IOs, CISOs, General Counsels, CCOs, CPOs and CMOs from US companies showed the following results:

- **54%** reported that GDPR readiness is the highest priority on their data privacy and security agenda.
- Another **38%** said GDPR is one of several top priorities.
- **77%** plan to spend \$1 million or more on GDPR
- **54%** of respondents plan to de-identify European personal data to reduce GDPR risk exposure



EFFECTS OF GDPR ON EVENTS INDUSTRY

This is a question widely asked by the event professionals over the course of time since the GDPR came into limelight. The event industry has an upper hand in collecting and storing data of all the attendees of any event across the globe. To secure and safeguard the data of EU citizens, the government approved the General Data Protection Regulation.

The events being held after 25th May'2018 has already signed up for GDPR regulations i.e. any event planner who collects the data of EU citizens regardless of the event location is supposed to abide by the GDPR policies.

Event Planners or Event Planning Companies fall under the category of “controllers” but the vendors like sales, marketing, and event-tech people and so on are “processors” which makes Event Industry follow the GDPR policies.

Meetings, events, and exhibitions are a base of collecting innumerable data which is vulnerable to a security breach. The GDPR regulations have brought major changes in which the data is going to be collected for the event forms and ticketing procedure so it might not be used for unnecessary marketing purposes as well without getting the consent of the users. The consent also brings a clause of sharing the attendee's information with third-party organizations that may even be sponsors, vendors or tech providers.

Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below

