THE LIVE LOVE LAUGH FOUNDATION
implementing
EU
General Data Protection Regulation (GDPR)
Agenda

Understanding GDPR

Why should we implement GDPR?

How do we implement GDPR?
Before we start

Go to https://thelivelaughfoundation.org

Identify all entry points of Data inflow

Get acquainted with these entry points with test data

What are the other entry points?
Teams
That have access to User Data

TLLLF
Data intake through:
1. Social media
2. Typeform
3. Google Analytics
Responsible for:
1. Content Creation
2. Content Publishing on Social Media

Ace Hacker
Data intake through:
1. Typeform
2. Google Analytics
Responsible for:
1. Cyber Security
2. Content Publishing on Website
3. Reporting
### Teams

**TLLLF**
- Data intake through:
  1. Social media
  2. Typeform
  3. Google Analytics
- Responsible for:
  1. Content Creation
  2. Content Publishing on Social Media

**Ace Hacker**
- Data intake through:
  1. Typeform
  2. Google Analytics
- Responsible for:
  1. Cyber Security
  2. Content Publishing on Website
  3. Reporting
What is GDPR?

General Data Protection Regulation

Regulation in EU law on:

Data Protection and Privacy

for all individuals within the European Union and the European Economic Area.

It also addresses the export of personal data outside the EU and EEA areas.
Why is TLLLFF concerned?

- Capturing EU user’s personal data
- Export of personal data outside of EU & EEA
Brexit?

Regulation in EU law on:

Data Protection and Privacy

for all individuals within the European Union and the European Economic Area.

It also addresses the export of personal data outside the EU and EEA areas.
Brexit?

Regulation on Data Protection and Privacy

Enforced in UK by Information Commissioners’ Office (“ICO”)
GDPR

Main Objectives

Rules relating to:

• Protection of natural persons with regard to the processing of personal data
• Rules relating to the free movement of personal data.

This Regulation protects:

• Fundamental rights
• Freedoms of natural persons

In particular their right to the protection of personal data.

The European Parliament adopted the GDPR in April 2016, replacing an outdated data protection directive from 1995. It carries provisions that require businesses to protect the personal data and privacy of EU citizens for transactions that occur within EU member states.

The GDPR also regulates the exportation of personal data outside the EU.
GDPR
Implementation

- No Official Auditing authority
- No Official Certification authority
- No Official Seal of Compliance

Internal Audit by the
Data and/or Technology Team
The GDPR leaves much to interpretation. It says that companies must provide a “reasonable” level of protection for personal data, but does not define what constitutes “reasonable.”
Why GDPR?

RSA Data Privacy & Security Report

RSA Security LLC is an American computer and network security company. RSA was named after the initials of its co-founders, Ron Rivest, Adi Shamir and Leonard Adleman, after whom the RSA (Rivest–Shamir–Adleman) public key cryptography algorithm was also named.

- Consumers’ awareness of data capture and breaches is growing, with 73% of respondents claiming to be more aware of data breaches compared to five years ago. No Official Certification authority
- Would boycott a company that repeatedly demonstrated that they have no regard for protecting Customer Data.
Data breach

Under GDPR, Data Controllers and Processors must supply a detailed report regarding any breach of personal data to their local Data Authority ‘without undue delay’, and where possible within **72 hours** of the breached party becoming aware of it.
Data breach

8/7/2018

Ace Hacker Technologies Pvt. Ltd - Mail - Data Breach [Action required]

Ace Hacker <connect@acehacker.com>
Data Breach [Action required]

David and Robert from Typeform <support@typeform.com>
Sat, Jun 30, 2018 at 1:48 AM
Reply-To: support@typeform.com
To: connect@acehacker.com

Hello,

My name is David Okuniev, and along with my co-founder and joint-CEO, Robert Muñoz, we’re writing to inform you that a data security incident has occurred within the Typeform platform. The incident compromised some of our customer data, and some data from your respondents.

On June 27, 2018, our engineering team discovered that an unknown third party gained access to our server and downloaded certain information, including some of the data your respondents provided via Typeform. We responded immediately and closed the source of entry. Our engineers are closely monitoring our platform, and we’ve found no evidence of any recurrence of the incident.

To date, our investigation has revealed that your account was compromised. Only some of the data provided by your respondents prior to May 3, 2018 was affected.

As a data collection company and service provider, maintaining the security and privacy of our customers' data is our top priority. As part of our rapid response to this incident, our team took a variety of measures to ensure the ongoing security of your data.

Because each customer’s typeforms are different, the data downloaded during this incident will vary by customer. You may want to communicate with your respondents to inform them of this incident. Please see the Q&A below for more info about this.

In addition to the steps taken to date, our team have launched a comprehensive review of our system security to identify ways we can further increase our security measures to prevent future incidents. After the review, our system will be more secure than ever before.

We take security matters seriously, and we sincerely regret that this incident occurred.

David Okuniev & Robert Muñoz
Co-Founders and Joint-CEOs of Typeform

What happened?
- We identified the breach at 14:00 CET on June 27th, and remedied the apparent cause of the breach at 14:30 CET on June 27th.
- We have since been performing a full forensic investigation of the incident to be certain that this cannot happen again. The risk of recurrence is now deemed low enough to send out this communication.
- The results that were accessed are from a partial backup dated May 3rd, 2018. Results collected since May 3rd 2018 are therefore safe and not compromised.

What do you mean by "compromised"?
In this case, "compromised" means that the attacker obtained access to your data and downloaded it from our servers. Unfortunately, this means that the attacker has partial data you collected prior to May 3rd.

How does this impact me?
All the responses you received prior to May 3rd from your respondents in the typeforms listed below are compromised.

What data was compromised?
The results accessed were from a partial backup dated May 3rd, 2018. As a result, all data collected since May 3rd 2018 are not compromised. Compromised typeforms are listed below.

What data is safe (i.e., not compromised by this incident)?
- Your subscription payment info is safe and secure (credit card, address, etc).
- Your typeform password is safe.
- The data you have collected since May 3rd is safe.
- If you collected payments via our Stripe integration, all of your audience’s payment details are safe.

https://mail.google.com/mail/u/0?ik=e6bdc4756a&jsver=SpEck3ZemTg.en.&cbl=gmail_fe_180801.14_p1&view=pt&msg=1644d3285358e927&q=from:connect@acehacker.com...
GDPR

Individual’s Rights over their Personal Data

Under GDPR, Individuals have extended rights over their Personal Data, including:

• The right to Data Portability
• To request a copy of any personal data held on them
• To request that their personal data is rectified
• To request that their personal data is deleted
Failure to comply with GDPR can result in a fine ranging from **10 million euros** to **four per cent of the company's annual global turnover**, a figure which for some could mean billions.

Fines will depend on the severity of the breach and on whether the company is deemed to have taken compliance and regulations around security in a serious enough manner.

The **maximum fine of 20 million euros or four percent of worldwide turnover** -- whichever is **greater** -- is for infringements of the rights of the data subjects, unauthorized international transfer of personal data, and failure to put procedures in place for or ignoring subject access requests for their data.

A lower fine of **10 million euros or two percent of worldwide turnover** will be applied to companies which mishandle data in other ways. They include, but aren't limited to, failure to report a data breach, failure to build in privacy by design and ensure data protection is applied in the first stage of a project and be compliant by appointing a data protection officer -- should the organization be one of those required to by GDPR.
# GDPR Approach

<table>
<thead>
<tr>
<th>Understand what Personal Data you process</th>
<th>Address Privacy at Every Level</th>
<th>Take a Risk-based Approach</th>
<th>Ensure your Approach is Blended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where is the data stored?</td>
<td>Privacy by Design</td>
<td>Risk, Data, Security, Compliance Teams must work together with line of business leaders to protect organization &amp; customer data.</td>
<td>Breach Response</td>
</tr>
<tr>
<td>Who in TLLLFF has access to it?</td>
<td>Business Level</td>
<td></td>
<td>Data Governance</td>
</tr>
<tr>
<td>How is it used?</td>
<td>Technology Level</td>
<td></td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Compliance Management</td>
</tr>
</tbody>
</table>
A data protection officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR).

Data protection officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.
GDPR

DPO | Responsibilities

DPOs are responsible for educating the company and its employees on important compliance requirements, training staff involved in data processing, and conducting regular security audits. DPOs also serve as the point of contact between the company and any Supervisory Authorities (SAs) that oversee activities related to data.

The DPO’s responsibilities include, but are not limited to, the following:

• Educating the company and employees on important compliance requirements
• Training staff involved in data processing
• Conducting audits to ensure compliance and address potential issues proactively
• Serving as the point of contact between the company and GDPR Supervisory Authorities
• Monitoring performance and providing advice on the impact of data protection efforts
• Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
• Interfacing with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information
GDPR

DPO | Responsibilities

DPOs are responsible for educating the company and its employees on important compliance requirements, training staff involved in data processing, and conducting regular security audits. DPOs also serve as the point of contact between the company and any Supervisory Authorities (SAs) that oversee activities related to data.

The DPO’s responsibilities include, but are not limited to, the following:

• Educating the company and employees on important compliance requirements
• Training staff involved in data processing
• Conducting audits to ensure compliance and address potential issues proactively
• Serving as the point of contact between the company and GDPR Supervisory Authorities
• Monitoring performance and providing advice on the impact of data protection efforts
• Maintaining comprehensive records of all data processing activities conducted by the company, including the purpose of all processing activities, which must be made public on request
• Interfacing with data subjects to inform them about how their data is being used, their rights to have their personal data erased, and what measures the company has put in place to protect their personal information
DPO is easily accessible by anyone from any team whenever needed.
Processing of Personal Data by competent authorities for the purposes of:

- The Prevention, investigation, detection or prosecution of criminal offenses or
- The execution of criminal penalties, including the safeguarding against and
- The prevention of threats to public security.

GDPR Regulation does not apply in these cases.
# GDPR

Lawful Processing

<table>
<thead>
<tr>
<th>Consent</th>
<th>Contract with Individuals</th>
<th>Vital Interest</th>
<th>Public Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>You can process personal data where the subject has given consent to the processing for one or more specified purpose.</td>
<td>You can process personal data, without consent, where required under a contract with the data subject. Eg. Employment contracts.</td>
<td>You can process personal data, without consent, if it's necessary to protect someone’s life. (very important to TLLLF). Example, calling a phone number when a user is threatening suicide.</td>
<td>Where you have a legal basis for processing. Remember “Demonstrable”.</td>
</tr>
</tbody>
</table>
GDPR

Principles

- Lawfulness, Fairness, Transparency
- Purpose Limitation
- Data Minimization - Credit Card processing, for example: Don’t collect Address when CC processing only requires First Name, Last Name, CC number, etc.
- Accuracy
- Storage Limitation and not “retain only as long as necessary”
- Integrity and confidentiality
You can process personal data WITHOUT consent, if you have a genuine and legitimate reason to do so that includes:

**Commercial benefit** - direct marketing, for example

But exception if your interests are outweighed by harm to the individuals’ rights and interests.
Consent is always necessary to process personal data.

FACT
Consent is one way to comply with GDPR, not the only way.
TLLLF needs to rely on consent!
GDPR

Consent

Required:

**Direct Marketing**

Using or sharing personal data in a way that is potentially intrusive or unusual - e.g. sharing data with a survey company, selling database.

**Transferring personal data outside of EEA** - else companies would just transfer data outside of EEA and claim no responsibility under GDPR.

The European Economic Area was established via the EEA Agreement in 1992, is an international agreement which enables the extension of the European Union's single market to non-EU member parties. The EEA includes EU countries and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU's single market. Switzerland is neither an EU nor EEA member but is part of the single market - this means Swiss nationals have the same rights to live and work in the UK as other EEA nationals.
GDPR

Consent

Not Required:
If you are in a **position of power** over the individual - Eg. Employer

Consent is a **pre-condition of using the service**.

You would still process personal data using a different basis **even if consent was withdrawn**. Eg. Machine Learning - your personal data has become a data point.
GDPR

Consent Statement on the website

“...any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”
GDPR
This is not consent

- Silence
- Pre-ticked boxes, or
- Inactivity

should **NOT** be used as indication of consent!

Eg. On the phone or email - no response to question of consent, Inactivity on the website
Identify basis of processing: Ensure consent is the most appropriate basis for the processing.

Clear and plain language: Use language that is easy to understand when obtaining consent. Avoid legal jargon!

Third parties: Give details of any third parties who will be relying on the consent.

Keep records: Who gave consent? When and how was consent given? Review consents regularly.

Withdrawal: Make withdrawal of consent straightforward and simple.
Don’t bundle consent: Keep separate from other terms.

Don’t make it a pre-condition of signing up to a service.

Blanket consent: Get separate consent for separate things where possible. Do not rely on a blanket consent.

Don’t use pre-ticked boxes: It should be an active opt-in.

Don’t rely on implied consent

Penalizing withdrawal: Do not penalize individuals who withdraw their consent.

Public authorities: Take extra care to show consent has been freely given. Avoid over-reliance on consent.
If we can’t easily explain what we’re doing with personal data then we shouldn’t be doing it.
Exercise

https://thelivelovelaughfoundation.org

• Identify all Data Entry points.
  ○ Verify Consent
  ○ Request Form to withdraw Personal Data
  ○ Privacy Statement
  ○ GDPR Audit Documentation
  ○ Escalation Matrix
  ○ Self Assessment
Gap

gdpr.thelivelovelaughfoundation.org
On the forms collecting data:
- **Terms and conditions**
- **Contact permission**: opt-in tick box
- **Keep in touch with us**: opt-in tick box

Through consent, you can gain insight into each individual’s interests to provide them with information that they want to receive.
Increase Trust

Personalized Emails *wherever possible* in place of Generic Emails
GDPR
Copywriting

- Write in plain English.
- Active voice
- Highlights the benefits
- Avoid personal pronouns
- Make future opt-outs clear
The Privacy and Electronic Communications Regulations (PECR) sit alongside the Data Protection Act and the GDPR. They give people specific privacy rights in relation to electronic communications.

There are specific rules on:

- Marketing calls, emails, texts and faxes;
- Cookies (and similar technologies);
- Keeping communications services secure; and
- Customer privacy as regards traffic and location data, itemized billing, line identification, and directory listings.