GDPR and ePrivacy

Compliance Nightmares for Open-Source Projects?

Giannis Konstantinidis

August 11, 2019

FrOSCon 2019

Presentation Breakdown

1. Introduction
2. Fundamental Aspects
3. Compliance Assessment
4. Common Mistakes
5. GDPR vs. ePrivacy
6. Additional Resources

Introduction

Background

- The EU GDPR, also known as Regulation (EU) 2016/679.
- Provides EU residents with additional controls.
- First published in April 2016; came into force on May 25, 2018.
- Repeals the former Directive 95/46/EC adopted in 1995.

Problem Statement

- This new data protection regime results into inequalities.
- SMEs are possibly expected to struggle with compliance.
- Decisive regulatory response if found to be non-compliant.

Fundamental Aspects

Essential Terminology

- Personal Data
- Special Categories of Personal Data
- Processing
- Data Subject
- Data Controller
- Data Processor
- Joint Controllers

Application Scope

- Material Scope
- Territorial Scope

Organisational Requirements

- Data Protection by Design and by Default
- Records of Processing Activities
- Technical and Organisational Measures
- Personal Data Breaches
- Data Protection Impact Assessment
- Data Protection Officer

Processing Requirements (1/3)

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality

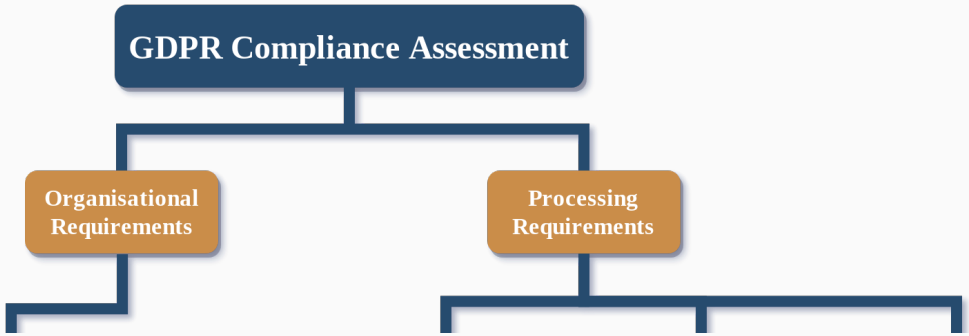
Processing Requirements (2/3)

- Consent
- Contract
- Legal Obligation
- Vital Interests
- Public Task
- Legitimate Interests

Processing Requirements (3/3)

- Transparent Information
- Right of Access
- Right to Rectification
- Right to Erasure
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object

Requirements Breakdown (1/2)



Requirements Breakdown (2/2)

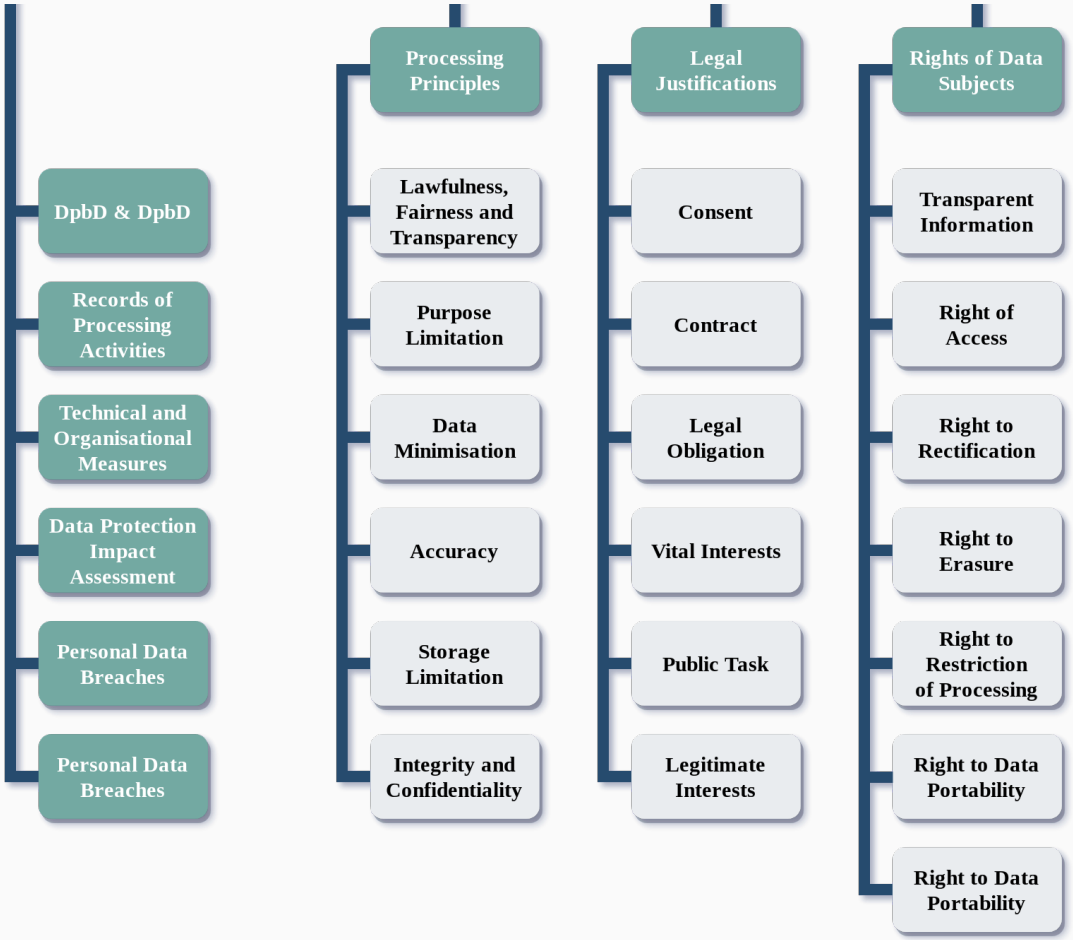


Figure 1: Breakdown of the Examined Requirements

Compliance Assessment

Analysis: Processing Activity (1/2)

- Processing Activity Name
- Controller Name
- Processor Name
- Processing Activity Description
- Storage Method

Analysis: Processing Activity (2/2)

- Data Type
- Legal Justification
- Security Measures
- Processing Principles
- Data Subject Rights

Analysis: GDPR Assessment (1/2)

Which are the roles of the organisation?

Does the organisation involve data subjects in the EU?

Has the organisation implemented appropriate measures?

Does the organisation maintain records of processing activities?

Analysis: GDPR Assessment (2/2)

Has the organisation published their privacy policy?

Does the organisation embrace DPbDesign and DPbDefault?

Has the organisation established a procedure for data breaches?

Has the organisation appointed a data protection officer?

Common Mistakes

Cookie Consent Banners (1/2)

Figure 2: Non-Compliant Banner

Cookie Consent Banners (2/2)

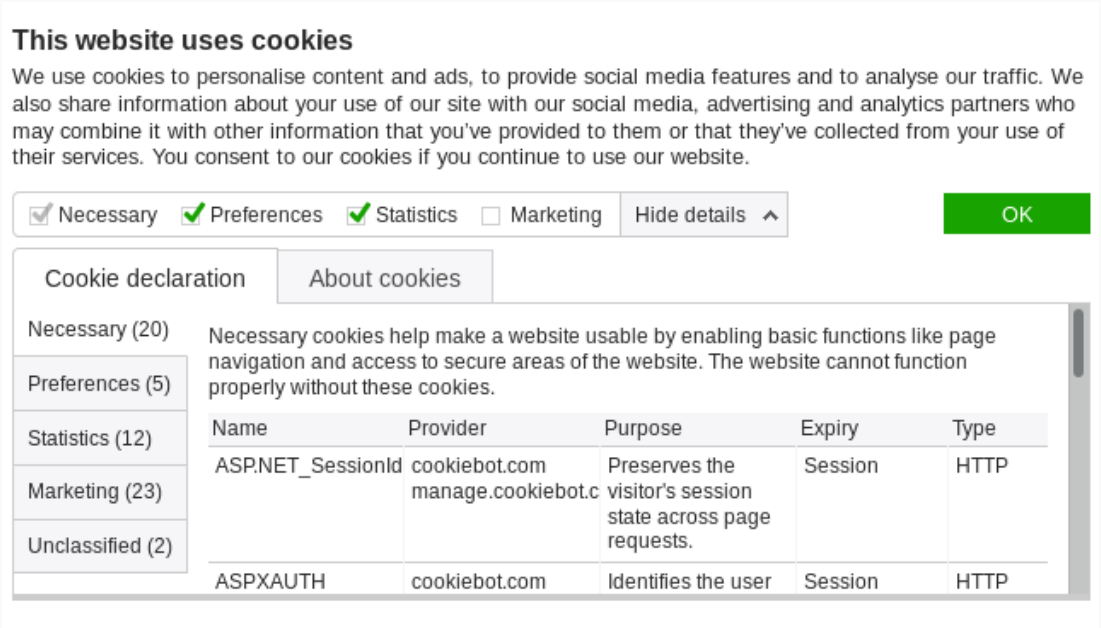


Figure 3: Compliant Banner

Sign-Up Forms

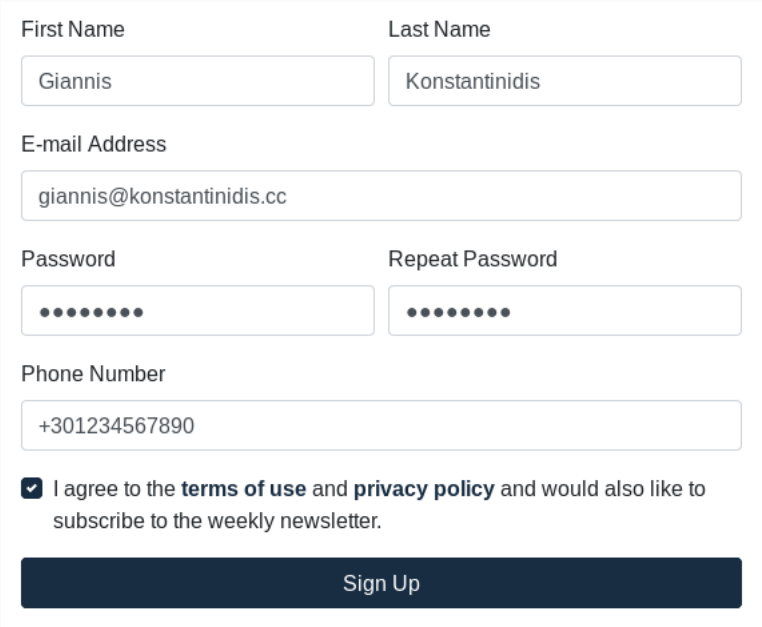


Figure 4: Non-Compliant Form

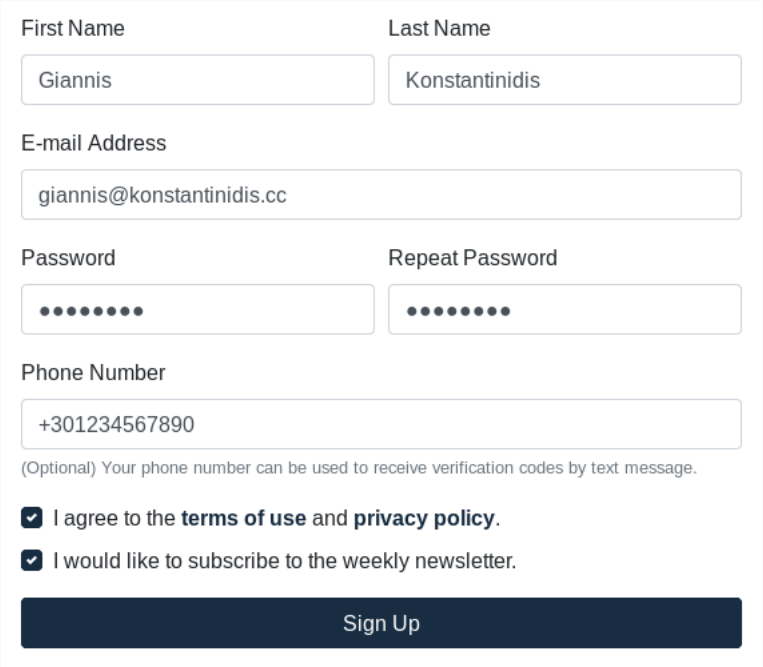
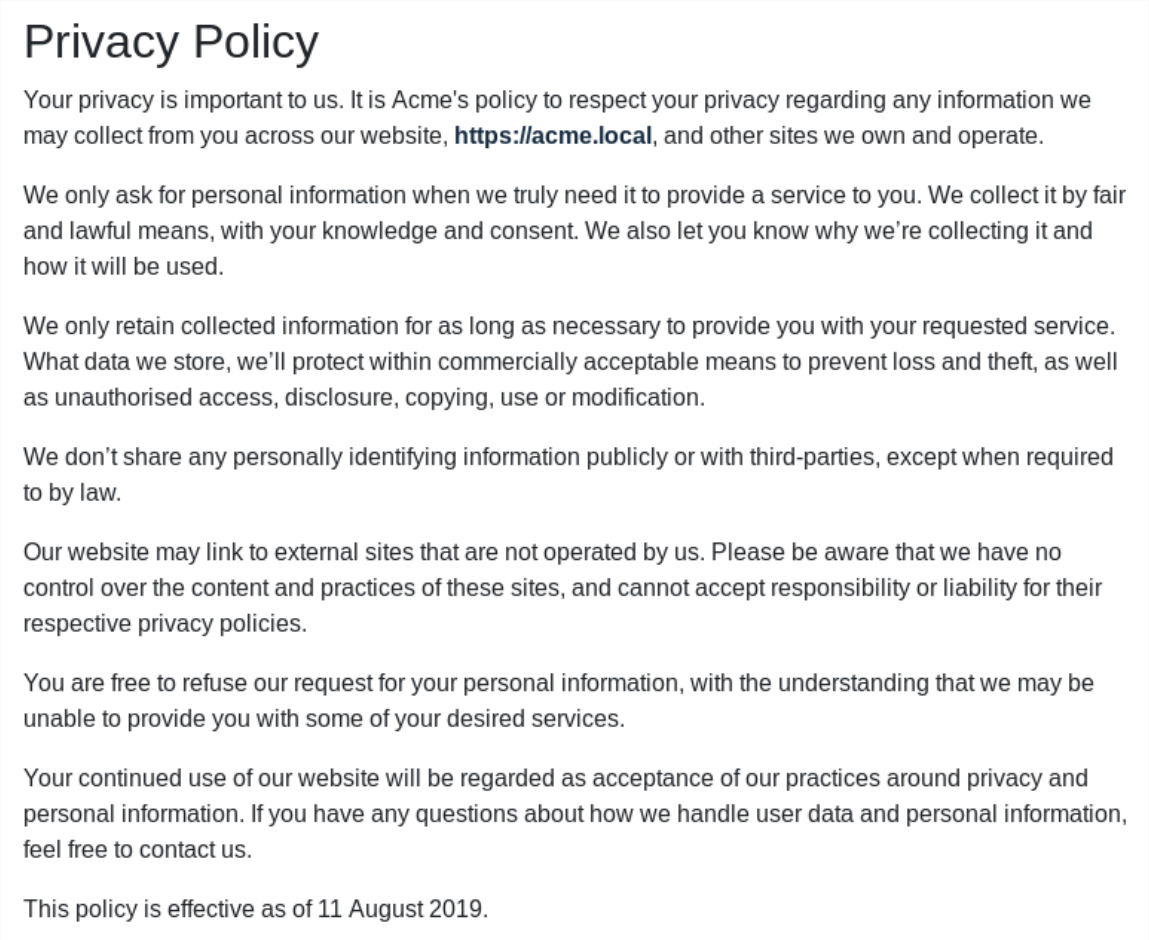


Figure 5: Compliant Form

Privacy Policies



Privacy Policy

Your privacy is important to us. It is Acme's policy to respect your privacy regarding any information we may collect from you across our website, **https://acme.local**, and other sites we own and operate.

We only ask for personal information when we truly need it to provide a service to you. We collect it by fair and lawful means, with your knowledge and consent. We also let you know why we're collecting it and how it will be used.

We only retain collected information for as long as necessary to provide you with your requested service. What data we store, we'll protect within commercially acceptable means to prevent loss and theft, as well as unauthorised access, disclosure, copying, use or modification.

We don't share any personally identifying information publicly or with third-parties, except when required to by law.

Our website may link to external sites that are not operated by us. Please be aware that we have no control over the content and practices of these sites, and cannot accept responsibility or liability for their respective privacy policies.

You are free to refuse our request for your personal information, with the understanding that we may be unable to provide you with some of your desired services.

Your continued use of our website will be regarded as acceptance of our practices around privacy and personal information. If you have any questions about how we handle user data and personal information, feel free to contact us.

This policy is effective as of 11 August 2019.

Figure 6: Non-Compliant Privacy Policy

GDPR vs. ePrivacy

ePrivacy Directive

- The ePrivacy Directive, also known as Directive 2002/58/EC. It was later amended by Directives 2006/24/EC and 2009/136/EC.
- Focuses on electronic communications and involves telephony, Internet and e-mail service providers.
- Acknowledges browser cookies, user-tracking, unsolicited communications and data retention practices.

ePrivacy Regulation

- The ePrivacy regulation would focus on particular issues.
- Expected to influence OTT and M2M communications, browser cookies and electronic communications for marketing purposes.
- May additionally involve non-personal data.
- The latest draft of the proposal was published on July 26, 2019.

Additional Resources

Useful Links

- GDPR Checklist: gdprchecklist.io
- GDPR Tracker: gdprtracker.io

Further Reading

- The GDPR and Firefox: mzl.la/2INKjlh
- Mozilla Privacy Policy: mzl.la/2Nx7OGk
- Things To Know About The GDPR: mzl.la/2A4v8Yv
- The Privacy Paradox Is A Privacy Dilemma: mzl.la/2Unkw1F
- Ready for GDPR: Firefox Focus Offers Additional Tracking Protection Against Advertisers: mzl.la/2Upqi2W
- Lean Data Practices: mzl.la/2TIqYUh

Questions?

Licensing