IT/Dev CONNECTIONS

GDPR Implications for your Application Environment Security

Andrew Baker
Virtual CIO & Technology Executive
BrainWave Consulting

Delivered by KNect365 TMT an Informa business

General Data Protection Regulation

…also known as **GDPR** or (EU) 2016/679

Title and reference

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

In force

ELI: http://data.europa.eu/eli/reg/2016/679/oj

General Data Protection Regulation

GDPR is primarily concerned with the data privacy rights of citizens of the European Union

2018 reform of EU data protection rules

Stronger rules on data protection mean people have more control over their personal data and businesses benefit from a level playing field.

PAGE CONTENTS

Rules for business and organisations

Application of the GDPR obligations, individuals' requests, enforcement

Rights for citizens

Protection of your personal data, your rights and redress

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

A key focus of GDRP is allowing EU citizens to be able to effectively manage any data that you have about them or are managing on their behalf

Nearly two months into GDPR, is the EU law making a difference?

With new GDPR-inspired US data privacy rules on the horizon and faster websites in the UK, the short answer is yes. But time will tell what its true impact is.

Robin Kurzer on July 16, 2018 at 8:30 am

For the past year or so, until the end of May, we were deluged with press releases from companies sharing opinions, predictions, innovations and more about Europe's General Data Protection Regulation (GDPR) and how it might affect businesses here and abroad.

GDPR is data privacy legislation that governs the handling of personal data from European Union (EU) members, even when they are in other countries such as the United States.

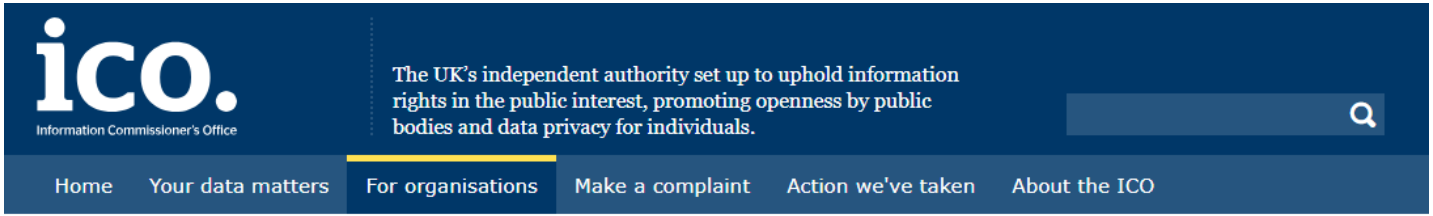
The May 25 deadline came and went, and since then, we've heard a lot less.

So, now we're wondering, nearly two months in, is GDPR having an effect?

Compliance continues to rise

https://martechtoday.com/nearly-two-months-into-gdpr-is-the-eu-law-making-a-difference-218226

Most of the focus on GDPR tends to center on “The Right to be Forgotten”



Most of the focus on GDPR tends to center on "The Right to be Forgotten"

https://www.businessinsider.com/google-fights-european-court-right-to-be-forgotten-expansion-2018-9

BUSINESS INSIDER

TECH | FINANCE | POLITICS | STRATEGY | LIFE | ALL

- Google is fighting a big battle in the European Union's top court about whether people's "right to be forgotten" should apply globally to its search engine.
- Private citizens in Europe can ask Google and other search engines to remove certain unflattering results about them.
- France's data-protection agency said that Google deleted results only from its EU search engines and that the information remained visible on non-EU domains.
- Google argued Tuesday that applying the rule globally would impinge on people's right to free expression.

https://www.businessinsider.com/google-fights-european-court-right-to-be-forgotten-expansion-2018-9

Most people outside Europe don't know much about the digital "right to be forgotten," the idea that private citizens can ask search engines to scrub certain results about them.

It's a comparatively new idea, but a landmark ruling in 2014 from the European Court of Justice set the initial parameters of how it might apply. That ruling said search engines like Google could be forced to delete results.

That ruling is at the center of a thorny battle between Google and France's data-protection agency, CNIL, which is arguing that the right to be forgotten should apply to search-engine results globally, not just within the EU.

The implications of GDPR and similar legislation, give developers and opportunity to look at the **security implications** of data privacy.

Opportunity vs Liability

Compliance, in general, and **GDPR**, in particular, offer organizations (and savvy technologists) an opportunity to improve their security posture.

Compliance is **not** the natural enemy of security…

GDPR Areas of Implication

- Data Access by Individual Subjects
- Data Reporting
- Data Backups & Retention
- Sanitizing Existing Records
- Tracking Compliance with Removal Requests

Questions We Need to Ask

How can I … … … in a way that facilitates all my business objectives, yet makes compliance easier?

… store customer data …

… allow individual data access …

… generate and manage backups …

… produce historical reports …

Data Access by Individual Subjects

- Customer data is often considered only in the aggregate.

- This makes it much harder to manage an individual data subject when necessary.

Data Access by Individual Subjects - ???

- How can I allow an individual data subject to easily request his or her data?

- How can I quickly allow a single data subject to see how and where their data is being used in my application?

Data Reporting for Individual Subjects

- Little consideration is given for providing a customer with access to only his or her own data, or providing a report to that data.

- This makes a part of the compliance very cumbersome and stressful

Data Reporting for Individual Subjects - ???

- How do I make it easy for my organization to generate a report on all the data we have of a single data subject?

- How can I provide this report, in a secure and timely way, to the subject?

Data Backups & Data Retention

- Backups are typically created at a server or global level

- Data Retention is usually global for all data or all backups, and designed to satisfy restore timeframes.

Data Backups & Data Retention - ???

- How do I get rid of one data subject from historical backups?

- How do I balance recovery with compliance?

- What backup methods should be considered in light of the above?

GDPR Application Considerations

- Ensure that privacy data is indexed and tracked on a unique key that is not username, email, etc

- Provide a **privacy** field as part of the contact record that facilitates reports and queries of this data

GDPR Application Considerations

- Your application should not break if some details about a data subject need to be scrubbed

- Your backups architecture and retention will likely need to be revamped.

GDPR Application Considerations

- Review all aspects of the data processing stream holistically

- Your ability to sanitize the data **in-place**, will greatly expand your options with regards to other processes like backups

GDPR Areas of Implication

- Consider how you will deal with the proof of satisfying a removal request.

Customer Service:

Please remove “Bob” from the system

Data Removal Conundrum

Fact 1 – You keep weekly backups for 26 weeks

Fact 2 – You have a policy to delete requested data within 30 days

Fact 3 – A data subject requests that their data be removed

Question – How will you handle your historical backups?

Data Retention Considerations

- Retention times <= 90 days

- Segregate EU backups from other regions

- Separate system recovery backups from privacy data backups

- Assume that you will have holes in your backups

Other Design Considerations

- Consider hashing rather than erasure

- “Forgetting” someone is permanent

- GDPR requests need to be tracked, but somewhat anonymously

- The system needs to track **how** subject data is used

Log Management Considerations

- Look at Log Management Holistically

- Log Access: **Need To Know Basis**

- Use tokens and other symbolic representations of privacy data wherever possible in logs

- Clean up those stray logs

Final Points

- Control Your Own Destiny

- Expect more privacy regulations like this, especially outside the USA

- This new reality can help us reduce typical breach vectors

Questions and Answers

e: ABaker@BrainWaveCC.com
t: @BrainWaveCC
w: about.me/Andrew.S.Baker