Designing for data protection

Heather Burns  /  WordCamp Dublin 2017
Who am I?

(I’m not quite sure myself)

- Designed first site in 1997 on Lynx via Unix telnet on dialup
- Full time professional web designer 2007-2015
- Now I write, speak, and consult exclusively on policy and legal issues impacting designers and developers
- IANAL nor do I play one on TV
WordCamp organisers are always this glamorous
GDPR overview

(what do you mean you skipped Claude’s talk)
<table>
<thead>
<tr>
<th>Assessment</th>
<th>Awareness</th>
<th>Documentation</th>
<th>Privacy Notices</th>
<th>Children</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engagement</td>
<td>Individual Rights</td>
<td>Subject Access Requests</td>
<td>Consent</td>
<td>Lawful Basis</td>
</tr>
<tr>
<td>Process</td>
<td>PbD and DPbD</td>
<td>Data Breaches</td>
<td>DPOs</td>
<td>International</td>
</tr>
</tbody>
</table>
State’s approach to data privacy is a national scandal

So deep are the problems that actions for damages may be brought and convictions quashed

Fri, Oct 6, 2017, 01:00

TJ McIntyre
“That law – the Communications (Retention of Data) Act 2011 – forces telephone companies and ISPs to log details of everyone’s communications and movements and to store that information for up to two years.

In Murray’s words it constitutes, a form of mass surveillance of virtually the entire population of the State, involving the retention and storage of historic data, other than actual content, pertaining to every electronic communication, in any form, made by anyone and everyone at any time ...

a vast amount of private information pertaining to the personal communications of virtually everyone in the State is now retained without the consent of those affected ...

Although routinely referred to in anodyne terms as ‘data’ or ‘retained data’, this vast store of private information touches every aspect of an individual’s private and professional communications profile over a lengthy period.”
This is an opportunity.

- To improve your internal processes...
- Maintain your competitive advantage...
- and protect your users in a time of massive social and political insecurity...
- So view it as a positive!
- It’s not about comply “or else” because “the law says so.”
- It’s about shifting the way you approach your work for the better.
Putting it into practice
Privacy by Design
PbD / DPbD

- Privacy by Design is not a wooly concept: it is a recognised development framework
- Devised in Canada in the 1990s
- GDPR requires the adoption and documentation of PbD and DPbD
- Here’s one I made earlier: https://www.smashingmagazine.com/2017/07/privacy-by-design-framework/
The seven PbD principles
A different way of working

Your workplace culture:

● Familiarise yourself with the basic principles of Privacy by Design

● Review your existing sites, apps, and processes for best PbD practice

● Educate all staff, from boardroom to reception, on PbD

Your development culture:

● Work to PbD standards

● If you don’t need it, don’t collect it

● Document your processes and the thought that went into them

● Create a Privacy Impact Assessment process for data-intensive projects
Data minimisation
CAN'T HAVE DATA BREACH

IF YOU DON'T HAVE DATA
Change your thinking

• Collect as little data as required
• Retain data for as little time as required
• Delete data when no longer necessary
• Document everything
Gaining consent
Consent must be...

<table>
<thead>
<tr>
<th>Active</th>
<th>Specific, freely given, and unambiguous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive</td>
<td>Not presumed from a pre-ticked box or inactivity</td>
</tr>
<tr>
<td>Granular</td>
<td>Real active choices, not take it or leave it</td>
</tr>
<tr>
<td>Unbundled</td>
<td>You cannot force consent for one thing to receive another</td>
</tr>
<tr>
<td>Named</td>
<td>You must inform the user what specific parties will get their data</td>
</tr>
<tr>
<td>Verifiable</td>
<td>Documentation or it didn’t happen</td>
</tr>
</tbody>
</table>
Designing for consent

https://catalogue.projectsbyif.com/
Privacy notices
Privacy for lawyers – not users

Annotated Example

We **generally** may share personal information we collect on the Site with **certain** service providers, **some** of whom **may** use the information for their own purposes **as necessary**.
Privacy for users – not lawyers

**GDPR reclaims privacy notices** as concise, transparent, and intelligible dialogues with your users.

Going forward, your notices need to be written in plain English. They need to contain certain kinds of information in a cleanly formatted manner. They need to give your users choices.

And everything you are doing with your users’ data - *everything* - needs to come out into the open.
All change for privacy notices

Ensure that yours are:

- Written in plain English, with no “legalese”;
- Broken down into clear sentences and short paragraphs;
- Contain granular, non zero-sum options;
- Not squeezed in with general terms & conditions

Ensure that you:

- Review the privacy notices of the third parties you sent data to, or receive data from;
- Contain all the information and any formatting required by @DPCIreland;
- Work with partners to ensure they are working towards compliance as well.
<table>
<thead>
<tr>
<th>Information required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The data itself</strong></td>
<td>What data is collected, how data is processed, how data is used</td>
</tr>
<tr>
<td><strong>Why you collect it</strong></td>
<td>Consent or lawful basis</td>
</tr>
<tr>
<td><strong>Who it is shared with</strong></td>
<td>Specific named parties, what you share and why you share it</td>
</tr>
<tr>
<td><strong>What rights users have</strong></td>
<td>Subject access requests, complaints</td>
</tr>
<tr>
<td><strong>Clear options</strong></td>
<td>For consent, individual rights, and subject access requests</td>
</tr>
<tr>
<td><strong>Your information</strong></td>
<td>Contact details for your business and your DPO</td>
</tr>
</tbody>
</table>
Privacy Impact Assessments
A simple PIA process

- A description of the data processing you are carrying out, including the legal basis for data processing;
- An evaluation of the necessity of the data processing;
- An evaluation of the proportionality of the data processing;
- A risk assessment regarding the data subjects;
- What measures you are putting in place to mitigate risk; and
- What security precautions you have taken
Technical and security safeguards
Information required

- Password hashing and salting?
- Data sandboxing?
- Automated updates?
- Responsible disclosure?
- Staff training and accountability?
- Mandatory data breach notifications?
- Penetration testing?
- Encryption at rest and in transit?
- Physical data security?
Here be dragons
#GDPRubbish

- Professional certifications
- “Accredited” courses
- Compliance plugins
- Consent panic
- Fines fines fines fines fines fines fines fines
  OMG fines fines fines fines fines fines fines fines
- “Compliance” as a possibility
What’s ahead

Further GDPR awareness
Regularly visit [https://gdprandyou.ie/](https://gdprandyou.ie/) for new guidance

the ePrivacy revamp
Warning: #drama ahead

Brexit
Yeah, so we’re kind of screwing things up for you. Sorry about that.
Become a privacy champion

- Audit everything
- Document everything
- Refresh everything
- Train everyone
- Challenge everyone
- Then do it all again

- Choose privacy-conscious partners and suppliers
- Make privacy your selling point, and use it
- Keep up with changing IE, UK, EU, and US developments
- Use GDPR as the starting point, not the end
Want to know more?
https://webdevlaw.uk/data-protection-gdpr

@webdevlaw  https://webdevlaw.uk