Open Web Application Security Project (OWASP)

Response to the ICO Data Sharing Code of Practice Consultation

Introduction

This official response has been submitted on behalf of the Open Web Application Security Project (OWASP) by the OWASP Global Industry Committee, following our own consultation process.

OWASP welcomes guidance documentation which disseminates good practice and helps organisations comply with relevant legislation, regulation and other mandates.

Detailed Response

The OWASP response only replies to two questions.

6. Is the code relevant to the types of data sharing your organisation is involved in? If not, which additional areas should we cover?

In "Technical Security" on page 15, there is no mention of websites, yet these are one of the common channels that lead to personal data breaches. Our suggestion would be to add an item: *"If personal data is collected or processed using a web product (e.g. website, web application, mobile application), have the most common security risks been identified, removed or mitigated?*". In other words, have the security aspects of privacy protection been considered at an early stage of the development/acquisition process?

This could reference as footnotes, or in other supporting materials, the following free and regularly updated guidance documents:

- OWASP Top Ten - The Ten Most Critical Web Application Security Risks and further guidance contained therein http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- WASC Threat Classification http://projects.webappsec.org/Threat-Classification
- CWE/SANS TOP 25 Most Dangerous Software Errors http://www.sans.org/top25-software-errors/

10. Is there anything else you think the code should cover or are there any other ways in which you think the code could be improved?

In "technical security" on page 15, we believe "is your information encrypted" is too simplistic. Many difficulties exist in implementing encryption properly and problems can be introduced in unexpected ways. Whilst we understand this document cannot provide all the detail required, a better question would be "How is encryption implemented and managed?"

On page 17 in the discussion of data standards, non-Latin characters are mentioned, but the more generic issues of encoding (e.g. UTF-8) and escaping are not. These are significant factors in successful data sharing and for ensuring the integrity of the data once it has been exported from one system and imported into another. If not properly defined and implemented, data that is correct and safe in one system might become corrupt (inaccurate) or actively exploit a weakness in another leading to data loss, damage, destruction, etc (e.g. by SQL injection). Our suggestion is to add after "capabilities of its system.", a new sentence "*Ensure the data are correctly encoded and escaped when output so they can safely be used by the receiving system.*".

About OWASP

This official response has been submitted on behalf of the Open Web Application Security Project (OWASP) by the OWASP Global Industry Committee, following our own consultation process.

OWASP is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security "visible," so that people and organisations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.

OWASP has three active chapters in the UK (London, Leeds/Northern and Scotland). We also have one board member and three global committee members based in the UK. Further information:

- OWASP Foundation
  http://www.owasp.org/index.php/OWASP_Foundation
- About The Open Web Application Security Project
  http://www.owasp.org/index.php/About_OWASP
- OWASP Global Industry Committee
  http://www.owasp.org/index.php/Global_Industry_Committee
- National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice citing OWASP and it's documents
  http://www.owasp.org/index.php/Industry:Citations

OWASP and OWASP UK are listed in ENISA's Who-Is-Who Directory 2010.