Web Security and Privacy for Novices – Part 3

Backups, Data Security, and GDPR Compliance

Artur Lupp*, Alexander G. Mirnig* and Manfred Tscheligi†
*Center for Human-Computer Interaction
University of Salzburg, Salzburg, Austria
Email: firstname.lastname@sbg.ac.at
†Center for Human-Computer Interaction &
Austrian Institute Of Technology, Salzburg & Vienna, Austria
Email: firstname.lastname@sbg.ac.at

***Abstract*—In this paper, we present four patterns for nonprofessional web developers. This is the third part of a series of three thematically connected papers. The patterns in this part of the series address backups, secure data storage and the European General Data Protection Regulation. The reader will be introduced to the basic knowledge of backups, followed by an introduction to the new data protection regulations with an explanation how to handle the associated additional responsibilities regarding the handling and storage of personal data in the internet.**

Keywords–Patterns; On-line; Security; Privacy; Novice Users.

I. INTRODUCTION

With the aid of guides and simple to use programs, setting up websites, web shops, blogs and other web presences is as easy as it ever was. The problem is however, the lack of knowledge transfer about web security and privacy. Nonprofessional web developers setting up web shops without proper knowledge about the EU General Data Protection Regulation (GDPR) [1] may face charges for not obeying the European law when it comes to safe data storage or data handling. Even the lack of certain pieces of information on a commercial website can lead to irreversible financial data. Thus, blindly trusting in guides is a bad idea. This is one of many reasons why we decided to create web security and web privacy themed design patterns to aid nonprofessional web developers and to help to make the internet a safer place.

This paper constitutes the third part of a series of three thematically connected papers, describing patterns from the same pattern collection. The contribution of this paper is an additional set of four patterns addressing backups, safe and GDPR compliant data storage and GDPR compliance in general. The first paper of the three thematically connected papers contains two meta-patterns. The second paper provides a set of four patterns addressing updates, mail servers and the security of web shops. Section II provides a short overview over related word, Section III introduces four patterns with the titles: ”When and how should I create backups?”, ”How do I store data securely?”, ”Which data am I allowed to save?” and ”What information do I have to provide to visitors of my website?”. We will conclude this paper in Section IV.

II. RELATED WORK

On 25 May 2018, the new GDPR was applied across the European Union, enforcing new legal requirements as a necessity to get data controllers to protect personal data even more than before. However, data controllers are now confronted with new challenges, to ensure the safety and to comply with the GDPR. Two legal requirements which are very important prove themselves as very controversial [2]–[4]. The first one is the right to be forgotten and second the right to withdraw consent. In the era of big data, cloud computing and the Internet of Things, these laws might yield unforeseen problems and consequences depending on interpretation and implementation, especially for nonprofessionals in law and web development as shown by Alnemr et al. [5] and Bob Duncan [6]. Especially the right to be forgotten has a heavy impact on backups and their archivation [7]. Due to this circumstances operating websites, especially when handling and working with personal data might prove as challenging for novices in web development.

III. PATTERNS

A. When and how should I create backups?

Intent: Creating regular backups can make your life easier and less frustrating. Accidentally deleted, compromised or lost files can easily be restored trough backups instead of being lost forever.

Problem Statement: If files are deleted from a server, they usually are irrevocably lost. There is no recycling bin to store the deleted files in case you want to recover them. Corrupted or compromised files and database entries can render a website inoperable and in some rare cases they might even destroy the whole website. In cases like these, backups can be a life saver. A web shop for example that is offline for too long, due to missing backups or faulty data, can lead to significant financial losses. Apart from that, on-commercial websites that are offline for a longer period of time, will notice a drop in the rankings of searching engines.

Scenario: System relevant files were deleted due to a system error. The functionality of the website is greatly limited. After fixing this problem with great effort because no backups were available, you decide to inform yourself about backups.

Solution: Backups are, in simple words, basically duplicated version of (all or certain) files. A modern website consists of multiple files ranging from files that contain the design and style information, images, plugins and database files where the posts and comments of users are commonly saved. The best way to make a copy of all of those files is to create a (full) backup. There are multiple ways to create backups - either you create them manually by copying the

 ISBN: 978-1-61208-708-5

files one by one, or you use an automated script, a plugin or a special backup software. However the backups are made, you should always keep in mind that things can go wrong. Therefore, it is mandatory to understand the backup process in order to avoid mistakes and it is even more important to validate the backups after they are created. A corrupt, faulty or not working backup is as good as having no backup at all.

Backup Frequency - **Backups** should be created in **regular intervals**. But especially before:

- (major)updated of the operating system or important(server) software
- before moving to a new server (e.g., migration)

There is no golden rule for the frequency of backups. Generally, it is up to you, to decide when it is the time to create a backup. You have to think about the **importance and amount of the data** and whether it is **worth the time creating a backup**. It is possible to save some time, and skip backups with the possible risk of minimal data loss in case something happens. It is important to find the **balance**.

A web shop or a well visited bulletin board lively and active community, should do **daily or real-time backups**, as a data loss could have a very high impact and could lead to financial consequences. For more information about web shops please refer to pattern: How do I secure a web shop and what should be taken into consideration? [8]. If the site in question is **only for information purposes** or if the website **does not receive daily input**, it is sufficient to backup the site **once a week**.

Speaking of backups, there are a lot of possible forms. It is possible to secure only parts (e.g., images, files or only the database) of a page, or to do a full backup (i.e., saving the whole website with all of its components). If, for example, you have a well-visited website with only few postings and comments, a **full backup** (all files and the database) should be done **once a week**. A backup of the database, containing the user postings and comments should be done in more frequently. **Two or three times a week** seem reasonably if the page is well visited and the user base is posting or commenting frequently.

Note, however, not every type of backup makes it possible to restore individual files. Therefore, each and every backup method has to be tested and verified before you start relying on a certain method.

Verification of Backups - Backups are important! In case of a unfortunate event or a disaster, they might help you to recover individual files or even a whole system. Since backups might be the last resort in critical moments, you have to be able to count on them. This is why all backups should be tested and verified if it is feasible.

- Test whether they are corrupt or functional.
- Verify whether the Backups can be used to recover a system or files.

Automated Backups - Backing up a system manually (i.e., copy and paste important files by hand) can take a long time, especially when it is a large and complex system. Therefore, it is recommended to use backup software which offers the possibility to automate the backup process. Examples of such programs can be found in the ”Examples” section of this pattern. Some hosting provider also offer automated backups in their offers. It is recommended to keep that in mind, in case you forgot to do backups by yourself. This might save your day.

File and Database Backups - Before going deeper into specific backup solutions, it is important to be able to distinguish between data/file backups and database backups. Because depending of the type of data you want to back up, the processes vary. A WordPress page will be used as an example to explain the differences in the backup process depending on what is going to be saved.

Files: Apart from the mandatory main installation files of a WordPress installation,the term files also includes themes, designs, plugins, images, scripts (e.g., JavaScript, PHP, etc.), as well as other files and static pages. The files can be saved by following methods:

- Files may be backed up by the hosting providers (if they offer this service).
- Special backup software (e.g.,https://winscp.net/eng/docs/introduction) can create backups of your site and store them either locally or on a different server.
- There are WordPress plugins that create backups automatically at a certain time you can define (https://wordpress.org/plugins/updraftplus/).
- Manually transfer data to your own computer or a hard drive using a FTP (File Transfer Protocol) program (e.g.,https://filezilla-project.org) or command line tools.

Basically, its about saving files from one location and then copying them to a different location or storage device.

Databases: Database backups work differently compared to file backups. However, a database backup is always done the same way. Even automatically generated database backups by WordPress plugins, are identical to those that have been generated manually. First of all, you have to access the database by logging into it by using the database login credentials. Then you have to select the database entries you want to save and export them. This will result in a file, that can be used to recover the database entries. In the case of standard WordPress and phpMyAdmin installations, the database is called ”wp”. Login into the database, select the database ”wp” and export its contents. Viola, there you have the database backup.

It is recommended to make about **3 backup copies** and store them in **different locations (e.g., hard disk, cloud or server)**. This will help to be safe in case one or two of the storage locations fail.

Examples: Backup Software - The following programs can be used to back up individual files or complete systems. Please follow the links provided below if you want to know how the software works and whether it is suitable for your needs.

- tar
  - https://wiki.ubuntuusers.de/tar/
- Bacula
  - https://blog.bacula.org/what-is-bacula/
- dump
  - http://www.willemer.de/informatik/unix/unixdasi.htm [ger]

References: Backing Up Your WordPress Site [9]

WordPress Database Backup Instructions [10]

Backing up Your Website: The Ultimate Guide [11]

 ISBN: 978-1-61208-708-5

What kinds of Google Penalties are there and what are the differences? [12]

MariaDB - Backup and Restore Overview [13]

MySQL - Database Backup Methods [14]

MariaDB - mysqldump [15]

How Often Should You Backup Your WordPress Sites? [16]

Keywords: Backup, Security Backup, Database, Data Files

B. *How do I store data securely?*

Intent: This pattern addresses the problems of the secure storage of user generated content and user data.

Problem Statement: The secure storage of data has to be handled according to the EU General Data Protection Regulation [1]. This is especially important if the data in question is personal data.

Scenario: A website is allowing its users to write comments and to upload data (images or similar). The comments and content have to be transferred and stored on the web server securely.

Solution:

- Keep your system and server safe and up-to-date.
  - An up-to-date system equipped with an up-to-date anti virus program and the latest (security) updates offers less attack vectors for cyber criminals.
- SSL/TLS Encryption Communication
  - An encrypted connection allows a secure data transfer and guarantees data integrity.
- Save Received Data in Anonymous and/or Encrypted Format.
  - Important information, like passwords, should never be stored directly in plain text. Encrypt the data before storing it in the database.
  - Some data may only be stored in **encrypted and/or anonymous form (e.g., personal data)**.
    - For more information, please refer to pattern: Which data I am allowed to save? [17].
- Define and Set Access Rights.
  - The fewer people have access to the data, the safer the data generally is.
  - Adjust access rights for users individually.
    - Everyone should only have access to files and folders meant for them.
- Database Backup.
  - It is not just about storing the data safely. Securing the stored data is important as well.
- Encrypted Backups.
  - Encrypting backups is an additional step to take to secure the data even more. While this is totally optional, an encrypted backup can make it much harder for unauthorized people to access the files inside of them.

Examples: Ensure Security Your System - An up-to-date system offers less attacking vectors for potential cyber criminals. It is mandatory to ensure the installation of the latest (security) updates. More about this topic can be found in pattern ”When and how often should I install updates?” [18]. Securing your own computer or server is only the first step to ensure a secured system. It is also necessary to secure the website itself. Pattern How do I check the security of my website?” [19] explains in depth how this can be done.

Ensuring Data Integrity - Pattern ”How do I encrypt the communication with my website? [20] explains how to enable an SSL/TLS encrypted connection (HTTPS) on your own website. With a secure HTTPS connection, the communication between the users web browser and the encrypted website is encrypted. This ensures, that all the data that comes from the user is really from him.

Encrypt Packed Data Backups (Example uses 7Zip)

- How to protect your ZIP-Archives with a Password? [21][ger].

How to Encrypt Passwords using PHP

- Password Hashing [22].

References: Backup & Recovery [ger] [23]

Function Reference/wp hash password [24]

WordPress Password Hash Generator PHP [25]

Keywords: Data Security, Encoding, Data Storage, Personal Data

C. *Which data am I allowed to save?*

Intent: This pattern addresses the question, what data you are allowed to save on your website and what there is to consider when doing so.

Problem Statement: With all the advances in web development, nowadays it is possible to gather a lot of data from website visitors. But what kind of data are you allowed to gather and save according to GDPR (EU General Data Protection Regulation) ?

Scenario: Website operators have to follow the new GDPR and are required to adjust their website to match these regulations.

Solution: **Attention: This pattern is not a legal advice! We addressed the GDPR (https://www.dsb.gv.at/gesetze-in-osterreich [ger]) and applicable data protection regulations during our research for the patterns, however, we are no legal advisors, nor are we lawyers or privacy experts. We shall not have any liability whatsoever for the accuracy, completeness, timeliness, or correct sequencing of the provided information.**

Current regulations for **files, links and general user content**:

According to the Austrian E-Commerce Act 17 (exclusion of responsibility for links) [26], the website operator is not responsible for the content of links posted on his site (by other persons), as long as he has no knowledge of content provides via this link. However, if the operator determines that the link contains or links to illegal activity or information (for example, a link to a movie or a song file), the link has to be removed immediately.

It is recommended to apply regulations and define whats allowed on the website or not in the form terms of services. The terms clarify which and whether content may be uploaded by users, or that if content is uploaded, the user has to have the appropriate usage rights for that content. **Attention :** Never write anything in the terms and service, that you simply can

not do! For example, **never specify that any content will be checked before it is posted on your website**. As this makes you liable for each and any content on the website, regardless who posted it. As this states, that you have checked and verified that link in general and have knowledge about its content. The operator of a website is also liable for the content of a link posted by an employee or a person who is supervised by the operator.

Special regulations for **personal data** currently described in the GDPR:

- Website operators have to ensure the security of personal data.
  - It is defined in the GDPR as Privacy by Design / Privacy by Default, meaning, that everybody must use appropriate technical measures and procedures (e.g., pseudonymization) to ensure data security.
- Users need to be informed. Especially about what happens with their data and how their data will be used. In addition, users must actively agree that data may be stored by teh website.
  - More information can be found in pattern:What information do I have to provide to visitors of my website? [27].
- Users have the right to have their data deleted (i.e., "the right to be forgotten").
  - For more information please refer to :https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Pflicht-zur-Berichtigung.html#heading__Recht_auf_Loeschung_ [ger].
- Storage, transfer and distribution of personal data is not allowed without the users consent.
- If working with personal data, it is required to document the processing activities.
  - More information on that topic can be found here: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html
- The Court of Justice of the European Union has ruled that both static and dynamic IP addresses are to be considered as personal data.

A comprehensive blog post about GDPR and blogs can be found here: https://datenschmutz.net/dsgvo-checkliste-fuer-blogs/

Examples: Data Privacy - Inform Users and get their Consent - Example of Google search page:

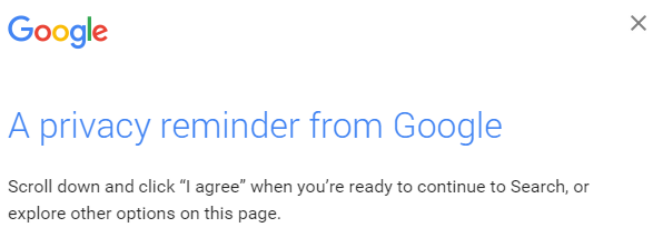

Figure 1. Google Privacy Reminder Info Page

A lot of companies changed their privacy and data regulations to address the GDPR. In reaction to that, Google and other companies informed their users of these changes. Figure 1 shows the reminder google used when users accessed the search page, listing and explaining what happens to the data collected by Google

You must actively agree to these conditions in order to be able to continue using Google without detours, as shown in Figure 2.

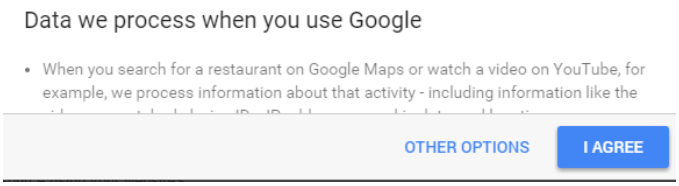

Figure 2. Google Privacy Reminder Info Page - Consent

What is personal data?

- General personal Data
  - Name, birthday date, age, address, e-mail-address, phone numbers, pictures from the person, education, job, marital status, nationality religious, as well as political attitude, sexuality, health data, holiday planning and police record.
- Identification (ID) numbers.
  - Social security number, tax number, health insurance number, ID card number, matriculation number.
- Banking Information
- Online Data
  - Internet Protocol (IP) address, a cookie ID, location data (for example the location data function on a mobile phone).
- Physical Characteristics.
  - Gender, skin color, hair color and eye color.
- Possession Features
  - Car, property ownership, land registry entries, license plate number.
- Customer data
  - Orders, bank account informations, account data, etc.
- Personal data can be defined as any information that relates to an identified or identifiable living individual. For example, a birthday alone can not always be linked to a specific person without additional information. However, if a name is added to this birthday, it is way easier to pin it down to a certain person. Thus, you have to be careful when displaying or providing personal data in general.

More information provided by the European Commission on Personal Data can be found here: What is Personal Data? [28]

References: Information about the GDPR provided by the Austrian Economic Chambers:

EU GDPR [29][ger]

EU GDPR - Data Security Measures [30][ger]

A blog post about user generated content [31][ger]

What is personal data? [32][ger]

 ISBN: 978-1-61208-708-5

Keywords: DSGVO, GDPR, Data Protection, Personal Data

D. What information do I have to provide to visitors of my website?

Intent: This pattern aims to inform website operators what kind information they legally have to provide their users on websites.

Problem Statement: The Internet is not a lawless place. There are laws intended to protect internet users which have to be respected by websites and theirs operators. Website owners should know their rights, as well as theirs responsibilities and should be at least be acquainted with the law.

Scenario: A website is almost ready to go online. What information does it have to provide to its users in order to be GDPR compliant?

Solution: **Attention: This pattern is not a legal advice! We addressed the GDPR (https://www.dsb.gv.at/gesetze-in-osterreich [ger]) and applicable data protection regulations during our research for the patterns, however, we are no legal advisors, nor are we lawyers or privacy experts. We shall not have any liability whatsoever for the accuracy, completeness, timeliness, or correct sequencing of the provided information.**

The website imprint, the terms of service and the privacy policy must be easy to find and access has always to be guaranteed. It is advisable to place these things in a good position where its visible all the time (e.g., in the header, or in the footer of a website).

Attention! - For web shops additional conditions apply. Please visit the following site for more information: General Terms and Conditions - Details [ger] [33].

- Imprint
  - The imprint is not an obligation for small private websites (e.g., a travel blog or a page only for friends). This is stated in Austrian Federal Law Consolidated Version, Media Act 24. Nevertheless, it is advisable to provide an imprint for the reasons of transparency.
  - The imprint includes:
    - Name or Company Name of the page owner and operator.
    - Registration number and place of registration.
    - Place of residence or registered office of the page owner.
  - If the site is serving (directly or indirectly) commercial purposes, the Austrian Federal Law Consolidated Version, Media Act 25 applies.
    - Disclosure obligation according to Austrian Federal Law Consolidated Version, Media Act 25 [34].
- Terms and Conditions
  - The terms and conditions should include the following:
    - A clear indication that users are responsible for the content of their posts.
    - Users have to agree to the terms if they want to use the website.
    - The posts from the users are not allowed to violate the terms or the applicable law.
    - The user holds the rights to his contents and contributions as long as it does not violate the law.
    - Contributions must not violate the rights of third parties (e.g., copyright, trademark law or personality rights).
    - Exemplary enumeration of content that should not be uploaded:
      - Copyrighted content, if no authorization exists (e.g., photos, images, videos).
      - Pornographic or adult content.
      - Racial, xenophobic, discriminatory or offensive content.
      - Content that violates applicable law.
    - Rules of conduct.
    - Restrictive measures and sanctions for violation of the terms of service.
    - Release from claims from third parties.
- Privacy Policy and use of Cookies:
  - Are cookies used at the website to save personal data or does the personal data general stored on the side (e.g., IP addresses)? Is there an information and an active consent requirement for site visitors?
    If cookies are used to save personal data (e.g., geo location) on a website, it is obliged to **inform the users and it is required to get an active consent from the users in order to be allowed to save the date**.
  - The use of cookies is only permitted if:
    - The user is informed in detail in advance.
    - Cookie use needs active consent from the user if saving personal data.
    - The consent must be given voluntarily, without doubt and through an active act.

Examples: Information for Storing Data (Including Personal Pata) - The patterns How do I store data securely? [35] and Which data am I allowed to save? [17] address the storage of data and person data.

Examples of Imprints and Disclosures

- https://datenschmutz.net/impressum/ [ger]
- https://www.wko.at/service/Offenlegung_Salzburg.html [ger]
- https://de.wikipedia.org/wiki/Wikipedia:Impressum [ger]
- https://www.guteguete.at/impressum [ger]

Example: Liability Disclaimer

- https://www.conrad.at/de/ueber-conrad/impressum.html [ger]

Example for ABG (General Terms and Conditions / Conditions of Use)

- https://www.amazon.com/gp/help/customer/display.html?nodeId=201909000
- https://www.amazon.de/gp/help/customer/display.html?nodeId=201909000 [ger]

Example: Privacy Statements / Policy

- https://policies.google.com/privacy?hl=en
- https://www.guteguete.at/datenschutzerklaerung [ger]

Example for a Cookie Notice for GDPR - See Figure 3 for an example of a Cookie Notice for European countries shown on https://www.nytimes.com.

 ISBN: 978-1-61208-708-5

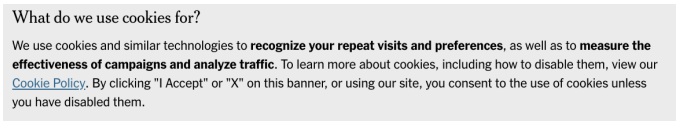

Figure 3. Cookie Notice shown on nytimes.com

Privacy Statement

- Sample of the WKO Privacy Statement [36][ger]

References: Establishment of an Online Store - Website [37] [ger]

Your own Website [38] [ger]

Austrian Federal Law Consolidated Version: Media Act 24, Version of 20.06.2018 [39] [ger]

Austrian Federal Law Consolidated Version: Media Act 25, Version of 20.06.2018 [34] [ger]

User Generated Content - Minimize your Liability [40] [ger]

Keywords: GDPR, EU, Personal Data, Privacy, Law

IV. Conclusion

This paper is the third and final part of a series of three thematically connected papers. It presents four additional patterns with the aim to aid nonprofessional web developers understanding common privacy and security problems frequently surfacing during the creation of websites. These patterns explain the importance of updates and the difficulties of saving and handling user data in a GDPR compliant way. While the explanation of the underlying concept and benefit of backups is quite straightforward and can easily be stated in one pattern, it is a different matter for the GDPR. Depending on the type of website and which data is being handled, the regulations and requirements defined by the GDPR can vary extremely. Thus, it is not possible to explain the complete GDPR in this format. We tried to cover the most important question by providing solutions, examples for possible problem cases in order to provide a decent knowledge base for novice web developers. Future work will mainly focus on the extension of the pattern solutions while keeping the existing patterns up-to-date to ensure future validity and usefulness.

Acknowledgment

The financial support by the Internet Privatstiftung Austria (IPA) under the program “netidee” with the title “SecPatt” under grant number 2390 is gratefully acknowledged.

References

[1] “EU General Data Protection Regulation (GDPR,” https://en.wikipedia.org/wiki/General_Data_Protection_Regulation, 2019 (retrieved April 10, 2019).

[2] E. Alepis, E. Politou, and C. Patsakis, “Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions,” Journal of Cybersecurity, vol. 4, no. 1, 03 2018, pp. 1–20, doi: 10.1093/cybsec/tyy001.

[3] C. Tankard, “What the gdpr means for businesses,” Network Security, vol. 2016, no. 6, 2016, pp. 5 – 8, doi: 10.1016/S1353-4858(16)30056-3.

[4] J. Krystlik, “With gdpr, preparation is everything,” Computer Fraud & Security, vol. 2017, no. 6, 2017, pp. 5 – 8, doi: 10.1016/S1361-3723(17)30050-7.

[5] R. Alnemr, E. Cayirci, L. D. Corte, A. Garaga, R. Leenes, R. Mhungu, S. Pearson, C. Reed, A. S. de Oliveira, D. Stefanatou, K. Tetrimida, and A. Vranaki, “A data protection impact assessment methodology for cloud,” in Privacy Technologies and Policy, B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, and S. Schiffner, Eds. Cham: Springer International Publishing, 2016, pp. 60–92.

[6] B. Duncan, “Can eu general data protection regulation compliance be achieved when using cloud computing,” in CLOUD COMPUTING 2018 : The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, ser. Cloud Computing 2018, B. Duncan, Y. Lee, and A. Olmsted, Eds. IARIA, 2 2018, pp. 1–6.

[7] E. Politou, A. Michota, E. Alepis, M. Pocs, and C. Patsakis, “Backups and the right to be forgotten in the gdpr: An uneasy relationship,” Computer Law & Security Review, vol. 34, no. 6, 2018, pp. 1247 – 1257, doi: 10.1016/j.clsr.2018.08.006.

[8] SecPatt, “How do I secure a web shop and what should be taken into consideration? [ger],” https://www.secpatt.at/patterns/pt_10/, 2018 (retrieved April 10, 2019).

[9] “Backing Up Your WordPress Site,” https://codex.wordpress.org/WordPress_Backups#Backing_Up_Your_WordPress_Site, 2019 (retrieved April 10, 2019).

[10] “WordPress Database Backup Instructions,” https://codex.wordpress.org/WordPress_Backups#Database_Backup_Instructions, 2019 (retrieved April 10, 2019).

[11] “Backing up Your Website: The Ultimate Guide,” https://webdesign.tutsplus.com/articles/backing-up-your-website-the-ultimate-guidewebdesign-4748, 2019 (retrieved April 10, 2019).

[12] “What kinds of Google Penalties are there and what are the differences?” https://www.sistrix.com/ask-sistrix/google-penalties/what-kinds-of-google-penalties-are-there-and-what-are-the-differences, 2019 (retrieved April 10, 2019).

[13] “MariaDB - Backup and Restore Overview,” https://mariadb.com/kb/en/library/backup-and-restore-overview/, 2019 (retrieved April 10, 2019).

[14] “MySQL - Database Backup Methods,” https://dev.mysql.com/doc/mysql-backup-excerpt/8.0/en/backup-methods.html, 2019 (retrieved April 10, 2019).

[15] “MariaDB - mysqldump,” https://mariadb.com/kb/en/library/mysqldump/, 2019 (retrieved April 10, 2019).

[16] “How Often Should You Backup Your WordPress Sites?” https://blogvault.net/how-often-should-you-backup-your-wordpress-sites/, 2016 (retrieved April 10, 2019).

[17] SecPatt, “Which data am I allowed to save? [ger],” https://www.secpatt.at/patterns/pt_9/, 2018 (retrieved April 10, 2019).

[18] SecPatt, “When and how often should I install updates? [ger],” https://www.secpatt.at/patterns/pt_1/, 2018 (retrieved April 10, 2019).

[19] SecPatt, “How do I check the security of my website? [ger],” https://www.secpatt.at/patterns/pt_7/, 2018 (retrieved April 10, 2019).

[20] SecPatt, “How do I encrypt the communication with my website? [ger],” https://www.secpatt.at/patterns/pt_4/, 2018 (retrieved April 10, 2019).

[21] “How to protect your ZIP-Archives with a Password?” https://www.heise.de/tipps-tricks/ZIP-Archiv-mit-einem-Passwort-schuetzen-So-geht-s-3907870.html, 2017 (retrieved April 10, 2019).

[22] “Password Hashing,” https://paragonie.com/blog/2017/12/2018-guide-building-secure-php-software#secure-php-passwords, 2017 (retrieved April 10, 2019).

[23] “Backup & Recovery [ger],” https://www.onlinesicherheit.gv.at/praevention/datensicherung_und_loeschung/datensicherung_und_wiederherstellung/249920.html, 2018 (retrieved April 10, 2019).

[24] “Function Reference/wp hash password,” https://codex.wordpress.org/Function_Reference/wp_hash_password, 2019 (retrieved April 10, 2019).

[25] “WordPress Password Hash Generator PHP,” http://www.kvcodes.com/2016/09/wordpress-password-hash-generator/, 2016 (retrieved April 10, 2019).

[26] “Austrian Federal Law Consolidated Version: E-Commerce Act 17, Version of 10.04.2019,” https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001703, 2018 (retrieved April 10, 2019).

 ISBN: 978-1-61208-708-5

[27] SecPatt, “What information do I have to provide to visitors of my website? [ger],” https://www.secpatt.at/patterns/pt_12/, 2018 (retrieved April 10, 2019).

[28] “What is Personal Data?” https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en, 2019 (retrieved April 10, 2019).

[29] “EU GDPR,” https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html, 2018 (retrieved April 10, 2019).

[30] “EU GDPR - Data Security Measures,” https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Datensicherheit-und-Daten.html, 2018 (retrieved April 10, 2019).

[31] “A blog post about user generated content,” http://www.rechtzweinull.de/archives/108-Haftung-fuer-User-Generated-Content-Grundsaetze-und-Hinweise-fuer-die-Praxis.html, 2009 (retrieved April 10, 2019).

[32] “What is personal data?” https://www.datenschutz.org/personenbezogene-daten/, 2018 (retrieved April 10, 2019).

[33] “General Terms and Conditions - Details,” https://www.wko.at/service/wirtschaftsrecht-gewerberecht/AGB_im_Internet_-_im_Detail.html, 2019 (retrieved April 10, 2019).

[34] “Austrian Federal Law Consolidated Version: Madia Act 25, Version of 20.06.2018,” https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000719&FassungVom=2018-06-20&Artikel=&Paragraf=25&Anlage=&Uebergangsrecht=, 2018 (retrieved April 10, 2019).

[35] SecPatt, “How do I store data securely? [ger],” https://www.secpatt.at/patterns/pt_8/, 2018 (retrieved April 10, 2019).

[36] “Sample of the WKO Privacy Statement,” https://www.wko.at/service/wirtschaftsrecht-gewerberecht/muster-informationspflichten-website-datenschutzerklaerung.html, 2018 (retrieved April 10, 2019).

[37] “Establishment of an Online Store - Website,” https://www.usp.gv.at/Portal.Node/usp/public/content/gruendung/gruendung_online-shop/website/Seite.70064.html, 2019 (retrieved April 10, 2019).

[38] “Your own Website,” https://www.help.gv.at/Portal.Node/hlpd/public/content/172/Seite.1720902.html, 2018 (retrieved April 10, 2019).

[39] “Austrian Federal Law Consolidated Version: Madia Act 24, Version of 20.06.2018,” https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000719&FassungVom=2018-06-20&Artikel=&Paragraf=24&Anlage=&Uebergangsrecht=, 2018 (retrieved April 10, 2019).

[40] “User Generated Content - Minimize your Liability,” https://www.it-recht-kanzlei.de/agb-user-generated-content-blog-forum-wiki.html, 2009 (retrieved April 10, 2019).

 ISBN: 978-1-61208-708-5