smashHit

Policy Guidelines

smashHit Platform Internal (Legal, Privacy, Consent) Policies Guides

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 871477

Introduction

The process/activity related Methodology Guidelines describes regulations in respect to the interaction between the key smashHit Stakeholders with the platform, such as contractual and privacy/security issues.

Purpose

The presented methodology guidelines cover legal, privacy and consent regulations for key processes/activities in respect to the actions/roles of the various stakeholders and their interaction required for the operation of the smashHit platform.

Audience

The methodology guidelines are meant for all stakeholders of the smashHit platform, as well as candidates planning to be a stakeholder.

Scope

The contents of the methodology guidelines will cover regulations in respect to the interaction between the various stakeholders.

The smashHit team does not take responsibility, when not following the instructions given in this guide.

If you find a regulation for which there is no content in this guide you can request it through info@smashhit.eu.

Troubleshooting

For any questions or inquiries about the use of the smashHit platform web application or the contents of it or this guide, or if you find there is no content in this guide for some functionality, please forward it to: info@smashhit.eu

Contact

smashHit Project website: https://smashhit.eu

smashHit platform support: info@smashhit.eu

Contents

1. Structure of the Guide

This guide is divided into two main parts. The first part looks at contractual regulations. It is meant to guide those who engage in digital or smart contracts within the infrastructure of smashHit.

The second part focuses on privacy and security issues around the processing of personal data. Here, the smashHit privacy policy is explained. It also contains important notes for data controllers who may wish to interact with the smashHit system.

At the end of this document, some frequently asked questions (FAQs) have been answered for readers, and in the Glossary key terms used within this document that might not be self-explaining or known by every reader are briefly explained.

2. Contractual Regulations

This part is meant to guide those who engage in a digital or smart contract within the smashHit system. A contract is simply an agreement between two or more parties that intend to produce a legally binding effect. Traditionally, a contract is entered into when one party makes an offer, and the other party accepts it. Other legal formalities may apply such as formality relating to the medium through which the contract is evidenced (e.g., in writing), or signature. Although the traditional contracting process is usually concluded manually, advancements in ICT have brought the opportunity to conclude some aspects of the contract process through automated means. This is commonly referred to as a "smart contract", "digital contract" or "automated contract".

Despite the technical developments, it is important to note that the digitalisation and automation of contracts has several legal implications and raises several questions such as whether automated execution of some or all aspects of a contract would produce a similar legal effect as a manually executed one; whether similar legal conditions applicable in traditional contracts are present in digital or smart contracts; whether the terminology used in designing digital or smart contracts has the same meaning when interpreted by the courts. At the core of this transition is the question of whether contracting parties seeking to regulate their mutual rights and obligations in a legally binding contract can use computer code (whether fully or partially) for this purpose. Other legal issues may arise relating to, for example, enforcement and termination. Careful consideration of these questions is very important for any actor engaging in smart contracting, particularly because of complying with legal requirements.

In the following, key elements, and requirements of entering a legally binding contractual relationship shall be explained in a nutshell.

2.1. Elements and Validity of a Contract

There is no harmonised contract law at the EU level. The following analysis is mainly based on commonly applicable rules across Europe. However, in some instances, national contract laws or principles are cited to emphasize specific points.

- **Creation:** a contract is created if: (a) the parties intend to be legally bound, and (b) they reach a sufficient agreement. A common model for the conclusion of a contract usually follows that an offer is made by one party, which is accepted by the other party or parties. Thus, all parties involved in a contract must express their agreement to the contract. Note that it is not in all cases and/or in all jurisdictions that certain formalities such as writing, or notarization are required to conclude a valid contract.

- **Content of the contract:** Contracts have elements that are mandatory with respect to their content. This requirement is related to the "certainty" of the contract, which implies clearly defining the contractual obligations of all parties and other elements such as the specification of the parties, the price, etc. For example, in a data sharing contract, the parties involved must be defined, as well as the subject matter of the sharing (the concerned data) and the conditions of the sharing, e.g., the price, the duration, among others. Where personal data is involved, the General Data Protection Regulation (GDPR; Regulation 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) further requires the parties to define the data protection actors – the data controller and data processor, and their responsibilities.

2.2. Digital contract

A digital contract is a contract, which is "entered into by two or more parties over an electronic communication line" (Weber, R. H., Contractual Duties and Allocation of Liability in Automated Digital Contracts, in: Schulze/Staudenmayer (eds.), Digital Revolution: Challenges for Contract Law in Practice, 2016, p. 163 (165 with further references)). Where such a contract is considered as information society services, Article 10 of the e-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market) requires certain information to be provided to the recipient of the service, including:

- The technical steps to follow to conclude the contract;
- Whether the contract will be filed and accessible;
- The technical means which are used to identify and correct preceding input errors;
- The languages offered for the conclusion of the contract; and
- Indication of relevant codes of conduct, including information on how to access these codes of conduct electronically.

In addition, the contract terms and conditions must be made available in a way that allows for storage and reproduction. If digital means replace contract documents in physical form, this has a further implication for the creation and management of the contract. For example, a traditional contract in writing is stored in a secure place for preservation and it is signed twice by both parties so that each party receives the same document. Such procedures aim at securing documentation of the contract and preventing subsequent alteration by one party. This should be replicated in a digital contract. Some commentators suggest storing the digital contract "on various redundant hard drives or media devices which enable retrievals" (Weber, R. H., Contractual Duties and Allocation of Liability in Automated Digital Contracts, in: Schulze/Staudenmayer (eds.), Digital Revolution: Challenges for Contract Law in Practice, 2016, p. 163 (181)).

2.3. Smart contract

A smart contract represents an automated way of executing an agreement. The UK's Law Commission (UK Law Commission, Smart legal contracts Advice to Government, November 2021, vii) defines a smart contract as "computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions". It is because of the self-executing nature of a smart contract that it is also referred to as an "automated contract".

There are several classifications of a smart contract. For example, Schrepel (Schrepel, T., Smart Contracts and the Digital Single Market Through the Lens of a "Law + Technology" Approach, European Commission, October 2021, p. 24-25) classifies it into three, namely: i) a smart contract combined with a "legal contract", i.e., a contract recognized by the law; ii) a smart contract without the support of a legal contract. iii) smart contracts combined with other smart contracts to create the conditions for the decentralized governance of (autonomous) ecosystems.

For a smart contract to be legally binding, all the elements required by law must be present in its creation and execution. Some legal reforms in the EU are addressing some issues relating to smart contracts, indicating some requirements to make such contracts secure. For example, Article 30 of the proposed Data Act (Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data, COM(2022) 68 final) contains some essential requirements regarding smart contracts for data sharing:

(a) robustness: ensure that the smart contract has been designed to offer a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

(b) safe termination and interruption: ensure that a mechanism exists to terminate the continued execution of transactions: the smart contract shall include internal functions which can reset or instruct the contract to stop or interrupt the operation to avoid future (accidental) executions;

(c) data archiving and continuity: foresee, if a smart contract must be terminated or deactivated, a possibility to archive transactional data, the smart contract logic and code to keep the record of the operations performed on the data in the past (auditability); and

(d) access control: a smart contract shall be protected through rigorous access control mechanisms at the governance and smart contract layers.

Furthermore, the vendor of a smart contract and other relevant actors shall perform a conformity assessment to comply with the essential legal requirements and issue an EU declaration of conformity thereafter. Adherence to EU harmonised standards in this area is also required, where such exist.

In summary, entities engaging in digital or smart contracts within the smashHit infrastructure must comply with the legal requirements relating to the formation of the contract, the content of the contract (its terms), security requirements, where applicable, rules relating to information society services, and any other requirements applicable within the relevant jurisdiction of the contract.

3. Privacy/Security Issues

Privacy, data protection and cybersecurity are important requirements that any actor in the information society must take seriously. In the EU, several rules have been made requiring data controllers, processors, manufacturers, and service providers to implement certain measures to protect not only the personal data they process, but also implement appropriate technical and organisational measures (TOMs) to secure their information systems. The GDPR, for example, includes several principles and obligations that data controllers and processor must comply with, which in a nutshell include:

- Observing the principles of data protection (Art. 5 GDPR)
- Complying with the various obligations applicable to the specific data processing operation, including record keeping, the appointment of a data protection officer, conducting a data protection impact assessment, adopting the data protection by design approach, and providing necessary information to the data subjects, among others.
- Facilitating the enforcement of the data subjects' rights
- Implementing appropriate data security measures, among others.

One transparency requirement is that data controllers and processors must have a policy that is publicly available to others who interact with them. The law also provides the content of certain information to be provided to the data subjects. Below, the privacy policy of smashHit is shown to inform those who interact with the platform, of the various measures adopted by the platform to comply with these legal requirements.

3.1. smashHit Privacy Policy

3.1.1. Preamble

smashHit provides an infrastructure comprising different modules including a consent management tool, a dispatcher, a contract support tool, a traceability module and security and privacy (S&P) mechanisms. These tools can process personal data for specified purposes.

The smashHit platform is designed according to the principles of privacy by design and by default in the meaning of Art. 25 GDPR to ensure that all processing of personal data within smashHit will comply with the applicable rules for the processing of personal data set by the GDPR.

This privacy policy provides relevant information to users of the smashHit system, particularly on how the system implements appropriate technical and organisational measures (TOMs) to ensure and be able to demonstrate that personal data processing is performed in accordance with the GDPR.

The policy contains information relating to the role of smashHit as a data processor.

3.1.2. smashHit as a data processor and its responsibilities

smashHit processes personal data on behalf of the data controller users of the smashHit system. These data controllers determine the purposes and means of the processing. smashHit acts as a data processor for the processing of personal data within the smashHit system.

Therefore, smashHit will implement appropriate technical and organisational measures to ensure and be able to demonstrate that all processing of personal data by smashHit is performed in accordance with the applicable data protection laws. Those measures will be highlighted below.

3.1.3. Personal data processed by smashHit

smashHit collects and processes the following data directly from the **data controllers** that use our system:

- email address of the data controller
- email address of the data subject who is in contractual relationship with the data controller.

We also collect the following data indirectly from the data controllers that use our system through a web browser:

- IP address
- Technical details from the devices used to access our system.

We also collect the following data indirectly when a data subject uses our system through a web browser:

- IP address
- Technical details from the devices used to access our system.

3.1.4. Purpose of data processing

smashHit uses the personal data provided to it under the applicable data processing terms with a data controller to confirm the information received by the controller on the processing and on the consent declaration by the data subject. This process is known as 'consent certification'. Subsequently, data is processed to provide data subjects with the ability to manage their consent.

3.1.5. Legal basis for data processing

The legal basis for the processing of personal data within the smashHit environment (where smashHit is a processor) is dependent on the relationship between the data controller and the data subject. For example, such legal basis could be a consent given by the data subject (Art. 6(1)(a) GDPR), or where the processing is necessary for the performance of a contract to which the data subject is party (Art. 6(1)(b) GDPR), or where the processing is necessary for the purposes of legitimate interests pursued by the controller subject to overriding interests of the data subject (Art. 6(1)(f) GDPR).

However, the relationship between smashHit and the controller is defined by the contract between these two actors (in accordance with Art. 28(3) GDPR).

3.1.6. Consent Management within the smashHit platform

smashHit provides a platform tool to simplify the process of consent for consumers to access data-based services. smashHit provides the necessary tools to display relevant information to the data subject concerning the consent he or she had granted, and to enable them to withdraw their consent should they wish to do so any time electronically via the consent management function and user interface. In case of consent withdrawal, smashHit will immediately inform all relevant parties that have been permitted to process the personal data by the consent.

smashHit does not store the document used to obtain consent. Such documents are kept by the data controller. smashHit however notifies the data controller when consent is withdrawn through the smashHit system.

3.1.7. Automated decision-making

smashHit does not process personal data for automatic decision-making that will produce legal effects on data subjects or similarly significantly affect the data subjects.

3.1.8. Duties of smashHit as a data processor

As a data processor, the GDPR imposes the following duties on smashHit:

- Record keeping

- processing only on the instructions of the data controller
- security measures, TOMs
- data breach notification
- at the choice of the controller, deletion or return of all the personal data to the controller after the end of the provision of services relating to processing, and deletion of existing copies unless Union or Member State law requires storage of the personal data
- making available to the controller all information necessary to demonstrate compliance with smashHit's obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

3.1.9. Data Subjects Rights

A data subject has several rights under the GDPR, such as:

- The right of access (Art. 15 GDPR): data subjects have the right to request from smashHit copies of the subject's personal data.
- The right to rectification (Art. 16 GDPR): data subjects have the right to request that smashHit corrects any information the data subject believes is inaccurate.
- The right to erasure (Art. 17 GDPR): data subjects have the right to request that smashHit erases subject's personal data, under certain conditions.
- The right to restrict processing (Art. 18 GDPR)
- The right to data portability (Art. 20 GDPR)
- The right to object to processing (Art. 21 GDPR)
- The right to avoid automated decision-making (Art. 22 GDPR).

Data subjects can exercise any of these rights by contacting: info@smashhit.eu

3.1.10. Cookies and how smashHit uses them

Cookies are text files placed on visitor's computer to collect standard Internet log information and visitor's behavioural information. When someone uses the smashHit web application, we may collect information from the visitor automatically through cookies or similar technology as follows: We use our own instance of the FIWARE identity manager "Keyrock"[1] to handle the authentication and authorisation of users. This instance of Keyrock makes use of three cookies: two cookies are used to keep the session (session & session.sig cookies), and a third cookie is a CSRF cookie (_csrf cookie). The CSRF cookie is used as a security measure to protect smashHit from cross-site request forgery attacks when using the session cookies. Apart from these, we do not use any other cookies.

3.1.11. Security of personal data

As specified in the data processing terms with the applicable data controller, smashHit takes reasonable and appropriate technical and organisational measures to protect personal data from loss, misuse, and inappropriate access. We use standard, industry-wide practices such as firewalls, encryption of data at rest and in transit, and (in certain areas) Secure Socket Layers ("SSL") to protect users' information.

3.1.12. Data retention and storage

Storage periods depend on the data processing terms with our data controller user and the individual data subjects. smashHit securely stores personal data as long as the terms of processing with the data controller permit.

3.1.13. Children

smashHit does not direct its data processing service to children.

[1] For information see https://fiware-idm.readthedocs.io/en/latest

3.1.14. Sharing with third parties

smashHit does not share personal data with third parties.

3.1.15. Transfer of personal data to third countries

smashHit does not transfer personal data to third countries.

3.1.16. Changes to our privacy policy

smashHit keeps its privacy policy under regular review and places any updates on its web page. This privacy policy was last updated in September 2022.

3.1.17. How to contact us

Any questions about smashHit's privacy policy, the data smashHit is processing about you as a data subject, or if you as a data subject would like to exercise any of your data protection rights, please do not hesitate to contact: info@smashhit.eu

3.2. Important Note for Data Controllers

3.2.1. Data controllers and their responsibilities

Users of the smashHit system as data controllers must ensure that all processing of personal data via their infrastructure has a legal basis. It is the responsibility of such data controller to identify the legal basis for processing. As data controllers, you are responsible for disclosing the rights of individuals and other information regarding the collection and use of their personal data, in accordance with the GDPR.

3.2.2. Information to be provided to the data subjects

Upon collection of personal data from data subjects, data controllers must ensure that they provide all the necessary information to the data subjects according to the GDPR.

3.2.3. Obtaining consent from the data subjects

As data controllers, you must obtain consent from the data subject and such consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject`s agreement to the processing of personal data relating to her or him (Art. 6 (1), Recital 32 of the GDPR). Data subjects must be properly informed about the purposes of the processing of their personal data in clear and plain language. Data subjects must be informed that consent can be withdrawn at any time by the data subject without any negative consequences for the data subject.

3.2.4. Establish a contractual relationship with smashHit as a data processor

Data controllers that engage the services of a data processor must establish a contractual relationship according to Article 28(3) of the GDPR.

In summary, entities acting as data controllers within the smashHit infrastructure must comply with the legal requirements imposed by the GDPR and other applicable regulations with respect to the collection, processing, storage, deletion or archiving of personal data, throughout the data lifecycle.

F.A.Q.

smashHit platform

Q: What is the smashHit platform?

A: smashHit is a platform that provides a generic, transparent way to view and manage consent certificates supported by disrupting technologies such as traceability of use of data, data fingerprinting and automatic contracting among the data owners, data provider, and service providers.

Q: How can I join smashHit?

A: In order to make sure the process is as straight-forward as possible for data owners, your registration in smashHit will be automatically handled by us when you sign your first consent with any of the approved smashHit partners.

Instructions to access smashHit will be sent to the email address you've indicated to the organization requesting consent.

Legal framework for contracts

Q: What do I need to comply with when engaging into a digital, smart or automated contract via smashHit?

A: Digital and automated contracts have several legal implications and raise several questions related to, e.g., the formation of such a contract, its content, and the security requirements to be complied with, see section 2 of this document.

Requirements of digital and automated contracts

Q: What are the key elements, and requirements of entering a legally binding contractual relationship via electronic means or with automated elements?

A: There are certain legal requirements related to the creation and the content of a contract as well as specific requirements depending on the concrete type and nature of the contract, see section 2.1 of this document.

Digital contract

Q: Are there any specific legal requirements for a digital contract and if yes, which?

A: Yes, there are specific legal requirements for digital contracts, see section 2.2 of this document.

Smart contract

Q: Are there any specific legal requirements for a digital contract and if yes, which?

A: Yes, there are specific legal requirements for digital contracts, they are described in section 2.3 of this document.

Relevance of privacy, data protection and cybersecurity

Q: What is the role of privacy, data protection and cybersecurity in the context of the smashHit system?

A: Privacy, data protection and cybersecurity play an important role as several instruments like the General Data Protection Regulation set rules for any actor in the information society, see section 3 of this document.

Role of smashHit with regard to privacy and data protection

Q: What is the role of smashHit in terms of privacy, data protection and security?

A: smashHit acts as a data processor, see section 3.1.2 of this document.

Information on details of processing and on the protection of privacy

Q: Where do I find information regarding the processing of personal data by smashHit, e.g. which data is processed by smashHit, how, for what purpose, and on which basis?

A: You will find such information in particular in the smashHit privacy policy in section 3.1 of this document.

Rights of natural persons

Q: What rights do I have as a natural person whose data is being processed by smashHit and how can I enforce them?

A: As a data subject you have a number of rights - see section 3.1.9 of this document, where you will also find information on what they imply, as well as contact details should you wish to exercise them. You will find information on how to contact us also in section 3.1.17 of this document.

Data controllers

Q: I am using smashHit as a data controller. Is there anything I have to observe?

A: Yes, it is important to know that as a data controller you have your own responsibilities, please see the respective note for data controllers in section 3.2 of this document.

Glossary

Automated contract: Contract or agreement which is executed automatically, see also → smart contract

Data controller: Legal term from the → GDPR - a body (e.g. a public authority or a company), which, alone or jointly with others, determines the purposes and means of the processing of personal data

Data processor: Legal term from the → GDPR - a body which processes personal data on behalf of a → data controller

Data subject: Legal term in the → GDPR used in a context where personal data is processed determining the person to whom an information is or can be related. The data subject is a natural person who can be identified, directly or indirectly, by a factor specific to her or his physical, physiological, genetic, mental, economic, cultural or social identity.

Digital contract: A contract concluded via electronic means

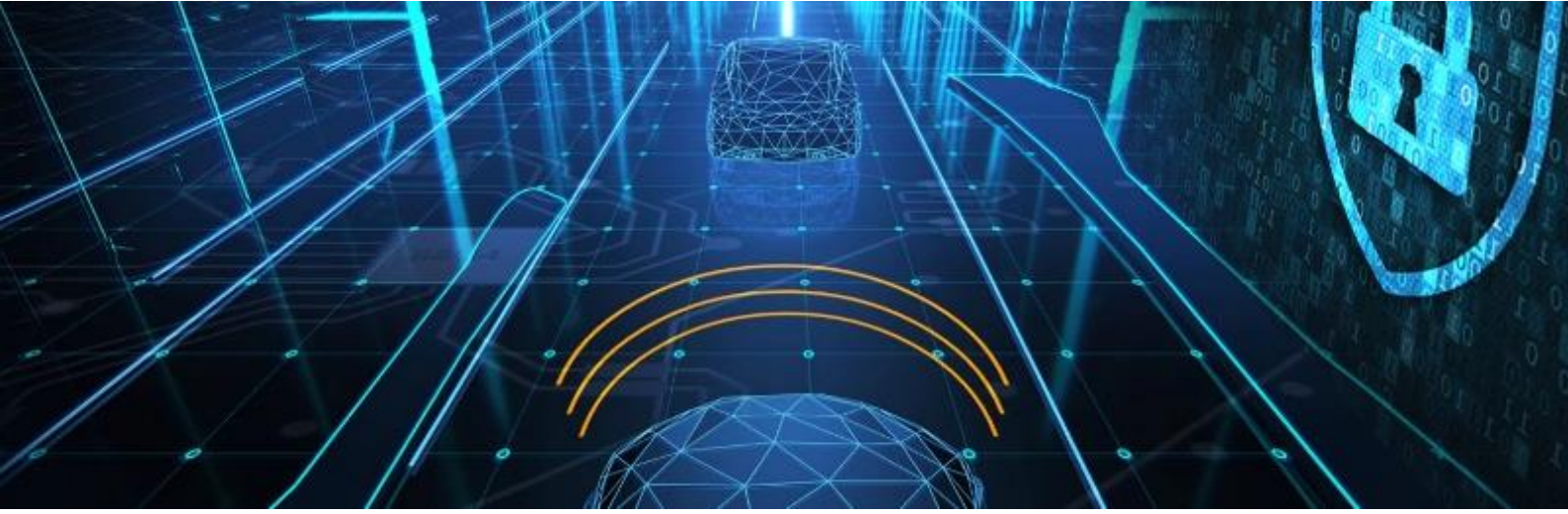
E-Commerce Directive: A legal norm on EU level to be transformed into national law by the EU Member States, laying down rules for electronic commerce related to information society services, e.g. the internet

GDPR: Abbreviation for 'General Data Protection Regulation', a legal norm on EU level adopted in 2016, which is directly applicable within its scope and lays down rules for the processing of personal data so as to protect natural persons' fundamental rights and freedoms, in particular their right to the protection of personal data

Personal data: Legal term in the → GDPR - any information related to an identified or identifiable natural person (see → data subject), e.g. a name or a home address

Smart contract: Automatic way of executing an agreement, in particular a contract, see also → automated contract

TOM(s): Technical and organisational measure/measures taken to ensure that processing of personal data is carried out in accordance with the rules of the → GDPR and to safeguard the rights and freedoms of → data subjects; the measures can be related to the security of the processing, e.g. the pseudonymisation or encryption of personal data



Our vision - Solving Consumer Consent & Data Security for Connected Car and Smart City

Further information

This document is part of the smashHit Methodology. The complete set of documents, including other user/developer guides as well as white papers created within this scope can be found on our website:

https://smashhit.eu/publications

Our consortium

Funded by the Horizon 2020 Framework Programme of the European Union