EPiC Series in Computing

Volume 93, 2023, Pages 152–163

Proceedings of Society 5.0 Conference 2023

Persona-oriented Data Protection Impact Assessment for Small Businesses

Bettina Schneider[1], Petra Maria Asprion[1], Ilya Misyura[1], Natalie Jonkers[1] and Esther Zaugg[1]

[1] University of Applied Sciences and Arts Northwestern Switzerland FHNW

bettina.schneider@fhnw.ch, petra.asprion@fhnw.ch, ilya.misyura@fhnw.ch, natalie.jonkers@fhnw.ch, esther.zaugg@fhnw.ch

Abstract

The European (EU) General Data Protection Regulation (GDPR) is applicable since May 2018 and has since posed major challenges for small businesses with limited knowledge and resources. According to Art. 35 of the GDPR, a so-called 'Data Protection Impact Assessment' (DPIA) is mandatory if a processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. There is a demand for low-threshold, practical instruments that support the required DPIA. The objective of this research was to develop a new DPIA instrument that meets the needs – as unit of analysis – of non-technology small businesses and complies with the requirements of the EU GDPR. Design Science Research was used as the methodological framework and identified personas were drivers in the development. The result is two variants of instruments that have been carefully evaluated and proven to be valuable.

1 Introduction

In our digitalised world, data has become the baseline for any business transaction. The processing of data implies the storage, collection, and usage of personal information. The EU GDPR, which is applicable since May 2018, is an essential means to ensure the protection of personal data, and hence the individual. So-called Data Protection Impact Assessments (DPIAs) are mandatory according to Art. 35 GDPR if the processing of personal data results in a high risk to the rights and freedoms of natural persons. In particular, the assessment is required before implementing a new technology (i.e., scanning fingerprints) that processes personal data. If a data breach occurs and is reported to the authorities, the incident will be subject to investigation. Non-compliance with GDPR - which includes a missing DPIA - can result in high fines (European Commission, 2020, p. 6). It is therefore important that companies independent from their size document that they have considered DPIA and can show evidence that a DPIA was conducted (GDPR, Legislation Regulation (EU) 2016/679, 2018, p. L119/53).

The implementation of the DPIA obligation for small businesses, which often suffer from limited resources and legal knowhow, is not trivial. Typically, the guidelines for conducting a DPIA are academic, law-oriented, and hence not sufficiently practical and intended for everyday use (Barnard-Wills et al., 2019, pp. 25, 31–32; European Commission, 2020, p. 10). Small businesses should seek advice from experts in case their experience is not sufficient; however, these services are associated with high costs. There is a demand for low-threshold assistance in implementing and operating GDPR and DPIA. Existing instruments serving as templates to conduct DPIAs adhere to standardised risk assessment practices. A conversion and simplification of these instruments towards a more practical solution would be a starting point to expand the previous academic and legal-oriented discourse towards the viewpoint of non-experts as is often found on this topic in small businesses.

The objective of this research is to develop a persona-oriented DPIA instrument that corresponds with the target group of small businesses and non-GDPR experts. The emphasis is on small businesses that do not offer technology-driven products or services and that do not have educated IT or data protection personnel. For them, data management is not their core expertise but still GDPR compliance is required. The result should support lay people or non-experts in assessing their data processing and in addition raising their data protection expertise in the GDPR framework.

The applied research approach refers to the design science research (DSR) model of Vaishnavi and Kuechler (2015, p. 15): problem awareness, suggestion, development, evaluation, and conclusion. DSR suits very well the objective of our research as the central outcome of DSR is an evaluated artefact, which can either be a first solution to a problem or an improvement of an existing solution (Hevner and Chatterjee, 2010, p. 5-6). As one method in the DSR framework, a literature review following Levy and Ellis (2006, p. 182) was conducted. It entailed a key word search using scientific databases (ABI Inform, ACM Digital Library, IEEE Explore, Web of Science, Scopus) and the web.

The result was an essential basis for the creation of so-called personas. A persona represents a fictional ´character´ with unique traits, different interests, likes, and dislikes. It is a user representation with the aim of improving decisions in development processes and addressing the needs of the target group (Chasanidou, Gasparini & Lee, 2015). Our literature-based personas were outlined by corresponding profile descriptions. In the suggestion phase, persona representatives were recruited for qualitative interviews to identify potentially high-risk data processing cases. These cases were used in later phases for applying the DPIA instrument we developed.

The literature review was also key to identify existing DPIA instruments. At the development stage, one expert interview was conducted to challenge the correctness of our artefact. The interviewee is a leading lawyer and data protection expert in Switzerland. His areas of expertise are data law, IT, and digital business. Moreover, the three iterations of evaluation based on qualitative empirical methods.

The remainder of this paper is structured as follows: First, the definition and procedure of DPIA derived from the literature is elaborated. Afterwards, selected existing DPIA instruments are analysed to determine the gap our solution shall address. The core of our paper describes the iterative development and evaluation our research artefact. Finally, a conclusion is drawn.

2 Background and Problem Awareness

2.1 Definition of DPIA

DPIA is defined as a procedure that describes the processing of personal data from individuals by assessing the necessity, proportionality, and risks of processing and defining measures to address these risks (WP29, 2017, p. 4). Compared to generic risk management procedures, the risk assessment in a DPIA does not focus on the risks of organisations in context with their activities but on the risks of individuals (Bieker et al., 2016, p. 24). The most important aspect in a DPIA is the characterisation of process logic and iteration (Dashti & Ranise, 2020, p. 310, Vemou & Karyda, 2019, p. 45). According to Bieker et al. (2018), a DPIA involves four phases (Table 1):

Phases	Description
Preparation	A team is defined that will carry out the DPIA and collect the relevant information. The threshold analysis is done if a DPIA is necessary. If the analysis concludes that a DPIA is necessary, the execution phase starts.
Execution	The risks and sources of risks are identified. The level of interference and protection is determined. Risks are evaluated and appropriate measures defined to mitigate these risks. The whole evaluation result is documented.
Implementation	The identified measures are implemented. The effectiveness of the measures is tested and evaluated. The steps are documented to demonstrate compliance with the regulation. Then the processing operations are approved.
Review	The risks for the rights and freedoms of natural persons are continuously reviewed. A DPIA or part of it is repeated if necessary. The DPIA process must be audited by an independent party if this is mandatory.

Table 1: Four Phases of DPIA to be compliant with GDPR Art. 5(2) (Bieker et al., 2018, pp. 208-209)

2.2 Procedure to Conduct DPIA

Figure 1 illustrates the necessary actions before, during, and after a DPIA is conducted according to Art. 35, 36, 39 and the recitals 74-77, 84 and 89-95. Art. 35(1) states that a DPIA must be conducted if the data processing results in a high risk to the rights and freedoms of natural persons, especially if new technology is implemented.

High risk is specified in Art. 35(3) as follows: Either when a systematic and extensive assessment of personal aspects related to individuals is conducted based on automated processing, or when special types of personal data (defined in Art. 9(1), 10) are processed on a large scale, or when systematic monitoring of publicly accessible areas is conducted on a large scale.

If the assessment indicates a high risk to the rights and freedoms of individuals, the DPIA must be initiated. Art. 35(7) defines the minimum requirements:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including the legitimate interest pursued by the controller – the organisation determining the purpose of the data processing (Art. 4),

b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes,

c) an assessment of the risks to the rights and freedoms of individuals,

d) the measures envisaged to address the risks, including safeguards, measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this regulation considering the rights and legitimate interests of the individual and potential other persons concerned.

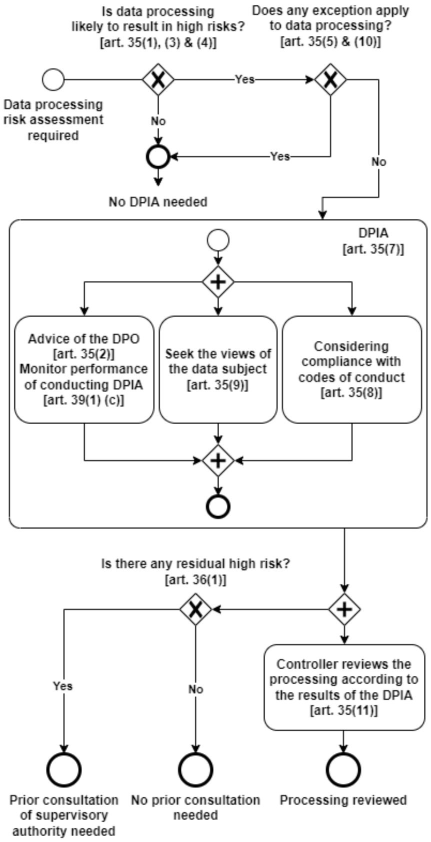

Is data processing likely to result in high risks? [art. 35(1), (3) & (4)]
Does any exception apply to data processing? [art. 35(5) & (10)]
Yes
Data processing risk assessment required
No
Yes
No
No DPIA needed
DPIA [art. 35(7)]
Advice of the DPO [art. 35(2)] Monitor performance of conducting DPIA [art. 39(1) (c)]
Seek the views of the data subject [art. 35(9)]
Considering compliance with codes of conduct [art. 35(8)]
Is there any residual high risk? [art. 36(1)]
Yes
No
Controller reviews the processing according to the results of the DPIA [art. 35(11)]
Prior consultation of supervisory authority needed
No prior consultation needed
Processing reviewed

Figure 1: DPIA Procedure (own figure based on WP29 (2017, p. 7))

When the DPIA implies that high residual risks occur, the controller must seek advice of the supervisory authorities before the data processing starts (Art. 36(1)).

The 'Article 29 Data Protection Working Party' (WP29, now 'European Data Protection Board' (EDPB)) defines in their guidelines concrete high risk data processing operations (WP29, 2017, pp. 9–11):1): Evaluation or scoring of individuals; 2) Automated decision making with legal or similar significant effect; 3) Systematic monitoring; 4) Sensitive data or data of a highly personal nature; 5) Personal data processed on a large scale; 6) Matching or combining datasets; 7) Data concerning vulnerable data subjects; 8) Innovative use or applying new technological or organisational solutions; 9) Processing preventing individuals from exercising a right or using a service or a contract. A data processing that meets at least two of the nine criteria indicates that a DPIA should be conducted. The more of the criteria are fulfilled by the data processing, the likelihood of a high risk to the rights and freedoms of individuals is higher and the more necessary it is to conduct a DPIA (WP29, 2017, p. 11).

The DPIA procedure described in GDPR is oriented towards larger companies that have employees responsible for data processing and data protection in place (e.g., Data Processing Officer (DPO) or Chief Information Security Officer (CISO)). For our new DPIA instrument, the mentioned division of roles and responsibilities is too exhaustive. Further, small businesses do usually not distinguish between a DPO, a CISO or other roles in this context; usually, the owner or appointed manager unites these roles. Hence, it can be concluded that the new DPIA instrument should not differentiate between roles and responsibilities as probably only one person conducts the DPIA. In case any support should be necessary during or after the DPIA, the small business must seek the advice of an external data protection expert. Compliance with relevant codes of conduct needs to be considered in a DPIA when assessing data processing. Codes of conduct are described in Art. 40(2) and include fair and transparent processing, the collection of personal data, and the information provided to the public and to individuals.

2.3 Existing DPIA Instruments

Most of the identified DPIA instruments from the literature search originated from the EU and are aligned to GDPR. To develop an effective solution tailored to a dedicated target group, the following selection was assessed in more detail [1]: 1) the 'sample DPIA template' from the United Kingdom (UK) authority Information Commissioner's Office (ICO, 2018), 2) the 'PIA software' from the French authority National Commission on Informatics and Liberty (CNIL, 2021), 3) the 'Data Protection Impact Assessment Threshold Analysis' by the Data Protection Authority of Liechtenstein (Datenschutzstelle Fürstentum Liechtenstein, 2020), and 4) the 'Guidelines on DPIA template' of the Information and Data Protection Commissioner (IDPC) of Malta (IDPC, 2020).

The first – the ICO solution – shows how to conduct and document a DPIA in seven steps: 1) identification of need for a DPIA, 2) definition of type scope and data processing, 3) stakeholder consultation, 4) necessity and proportionality evaluation of the data processing, 5) identification and assessment of risks, 6) identification of risk reducing measures, 7) signing and recording the DPIA result. The template builds upon a web-based, well-structured, and comprehensive documentation and as further benefit, the guidelines of the WP29 (2017) are incorporated. This documentation is organised in a Q&A-style and includes a list of examples of high residual risks. The DPIA itself can be documented in a Microsoft Word template, which is available for download.

The second – the PIA software from CNIL – proposes an open-source application to conduct a DPIA. Two versions are offered, one for download and one to be deployed on a server. The software is extensive and provides a step-by-step guide through the DPIA process with a visual interface. The DPIA is divided into four parts: 1) context, 2) fundamental principles, 3) risks and 4) validation. In the beginning, an overview is provided, then the data, processes, and supporting assets must be explained.

[1] Authors that compare existing (D)PIA approaches and were considered in this research are, e.g., Wright, Finn & Rodrigues (2013) or Grütter & Schneider (2019)

In context of fundamental principles, the proportionality and necessity of data processing are set out. During the risk part, planned or existing measures to ensure the data security must be listed (at least one). The final validation, approval, or rejection of the DPIA which refers to the review phase of the DPIA needs to be done manually by the DPO. A knowledge base is integrated and contextualises the information displayed in the instrument.

The third – the DPIA Threshold Analysis from Liechtenstein – offers a DPIA necessity check based on Microsoft Excel. The instrument is designed as a checklist for identification of need for a DPIA. It is not intended for conducting a complete DPIA. Nevertheless, the content is useful as it contains DPIA obligations and exceptions according to Art. 35 GDPR. Further, the high-risk factor categories mentioned in Art. 35 GDPR and in the guidelines of the WP29 (2017) are queried.

The fourth – the Guidelines on DPIA template from IDPC – includes minimal requirements of a DPIA and can be used and adopted to develop a simplified DPIA template very well suited for small businesses. The template is divided into eleven steps. The outcome of the DPIA, which is based on a downloadable PDF template can be signed by the DPO. The provided template offers marginal information or advice. However, the website further explains the DPIA process and related terms and refers to the WP29 (2017).

The analysis of the four instruments led to the following conclusions. The DPIA solutions from the UK (1) and Malta (4) are targeted at small businesses. Both solutions are document-based (Word, PDF) not providing embedded logic. For this reason, the evaluation of the assessment must be done manually. Both solutions are condensed and refer to external websites for supporting information. The very extensive instrument from CNIL (2) is offered as an open-source application. The adaptation of this instrument to realise a small-scale assessment would require some effort and skills. In addition, the assessment has a strong focus on data security measures, but still there is room for improvement like adding other risk categories, for example discrimination or the exclusion from a service. The solution of Liechtenstein (3) is built as Excel and generates the result based on macro-logic. As restriction, it exclusively offers the check whether a DPIA is necessary. No further information is provided on how the actual DPIA should be conducted. All four instruments follow the minimal requirements of a DPIA according to GDPR Art. 35(7) and the concept and steps of a DPIA mentioned in GDPR (cf. Figure 1). The procedures adhere to the high-risk categories defined in the guidelines of the WP29 (2017).

Overall, the presented DPIA solutions are to a certain extent scalable or explicitly recommended for small businesses. However, a DPIA instrument for non-technology small businesses that incorporates the necessary steps, essential low-threshold explanations and automatically generates a tailored assessment as a result could not be identified.

3 Suggestion, Development and Evaluation

3.1 Suggestion Phase

Our DPIA should be specifically adapted to the persona working in a non-technology small business, which does not have in-house IT experts and relies on software applications from third parties. Hence, our focus lies on small businesses using or implementing a (new) system/software from a third-party supplier or provider (e.g., third-party analytics software). In this situation, it should be verified whether a DPIA is necessary. Hence, our solution should start with a necessity check and if a DPIA turns out to be required, guide though the DPIA procedure. In case a supplier/provider already provides a DPIA for the provided software/system, this can be referred to. Nevertheless, a DPIA should still be carried out based on the specific utilisation in the context of the small business and its sensitive personal data.

To address the target group appropriately, the method of qualitative personas was utilised (Junior & Filgueiras, 2005, p. 281). This allowed us to limit the needs and to define a first group of beneficiaries.

Three personas were developed based on a literature review. We sharpened the developed profiles while allowing a reasonable spread (Table 2). To better understand the data processing of the personas, qualitative interviews were conducted with five persona representatives. The interviews prove that sensitive personal data is often processed in the tertiary sector, especially in health care. Personal data like names and addresses are processed regularly in the first and secondary sectors. The interviewees depend on providers for their infrastructure and systems/software when it comes to data protection. At the time of conducting this research, no third-party provider had yet advised the small business on how to comply with data protection regulations.

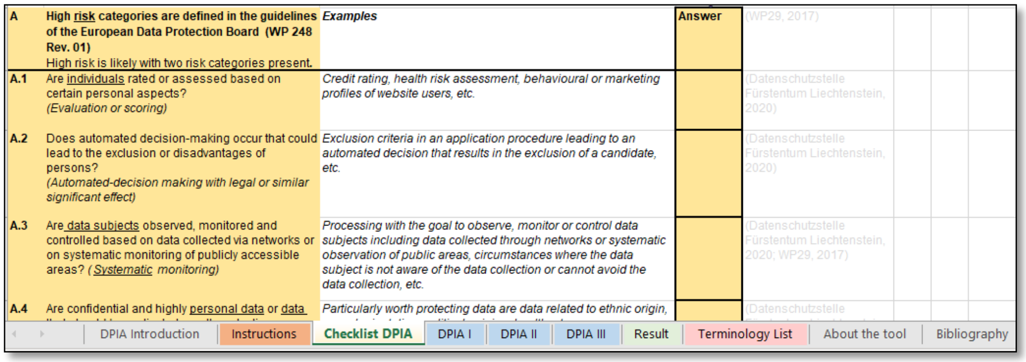
Persona	Economic sector	Data processing description
Organic farm with cattle farming and market gardening	Primary sector	Collecting sensitive personal data (name, date of birth, wages, etc.) from employees; collecting personal data from customers includes name and phone number which is stored in a physical address book. No electronic contact with customers in place yet but plans exist to switch to an Excel file and e-mail correspondence.
Brewery with brewery tours and courses	Secondary sector	Collecting sensitive personal data (name, date of birth, wages, etc.) from employees; personal data from private clients including name, address, e-mail address and phone number is stored locally on computer in several Excel files.
Pharmacy	Tertiary sector	Processing highly sensitive data (e.g., health data) from clients. Data processing is done locally on internal servers. Data is exchanged with the clearing office for health insurance via a secured connection. Prescriptions are sent by post to the clearing office for archiving purposes. Communication with doctors and hospitals takes place via phone or encrypted through a dedicated e-mail address of the pharmacy.

Table 2: Information about personas' data processing

3.2 Development and Evaluation Phase

Initially, our approach was implemented using a Microsoft Excel sheet as it is sufficient for prototyping, and as we avoid data collection from small businesses by offering them a downloadable Excel-based version.

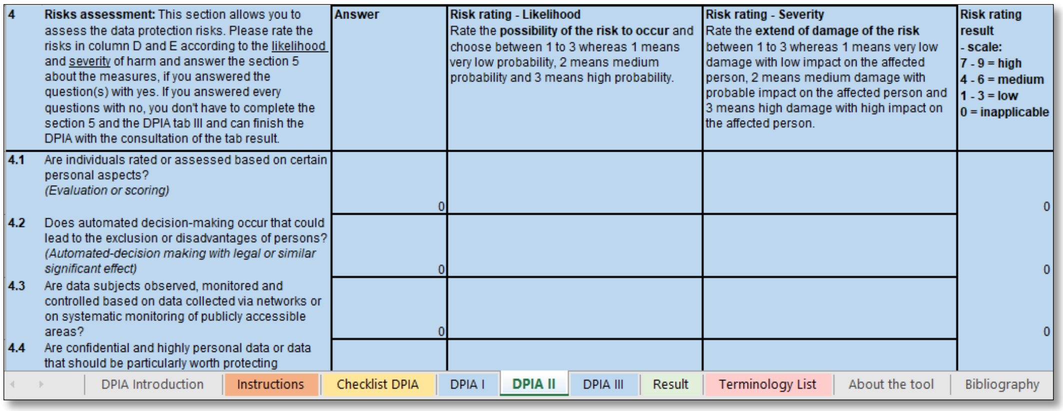
DPIA Instrument Version 1: The first version consists of ten tabs within Excel and seems at the first glance condensed and smooth. The structure follows the concept of a DPIA according to the GDPR and meets the minimum requirements. In more detail the structure looks like this: The first three tabs introduce the concept of DPIA (tab1), give detailed instructions for the approach itself (tab2), and check the necessity for a DPIA by a checklist assessing the data processing for high risk (tab3) (Figure 2).



A	**High risk categories are defined in the guidelines of the European Data Protection Board (WP 248 Rev. 01)** High risk is likely with two risk categories present.	*Examples*	**Answer**	(WP29, 2017)
A.1	Are individuals rated or assessed based on certain personal aspects? *(Evaluation or scoring)*	*Credit rating, health risk assessment, behavioural or marketing profiles of website users, etc.*		(Datenschutzstelle Fürstentum Liechtenstein, 2020)
A.2	Does automated decision-making occur that could lead to the exclusion or disadvantages of persons? *(Automated-decision making with legal or similar significant effect)*	*Exclusion criteria in an application procedure leading to an automated decision that results in the exclusion of a candidate, etc.*		(Datenschutzstelle Fürstentum Liechtenstein, 2020)
A.3	Are data subjects observed, monitored and controlled based on data collected via networks or on systematic monitoring of publicly accessible areas? *(Systematic monitoring)*	*Processing with the goal to observe, monitor or control data subjects including data collected through networks or systematic observation of public areas, circumstances where the data subject is not aware of the data collection or cannot avoid the data collection, etc.*		(Datenschutzstelle Fürstentum Liechtenstein, 2020; WP29, 2017)
A.4	Are confidential and highly personal data or data	*Particularly worth protecting data are data related to ethnic origin,*		(Datenschutzstelle

Figure 2 Screenshot from Version 1 – DPIA Necessity Check

The following three tabs (DPIA I, II, III) represent the actual DPIA in a series of questionnaires derived from the requirements for DPIAs defined in the GDPR and described in section 2.2 (Figure 3).



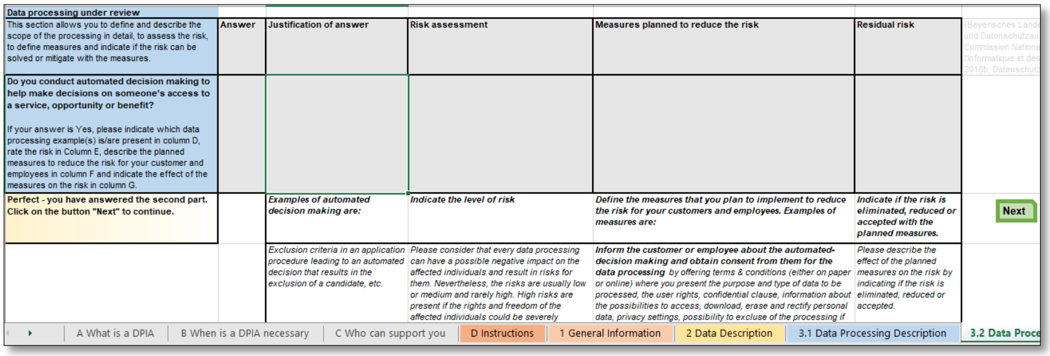
4	**Risks assessment:** This section allows you to assess the data protection risks. Please rate the risks in column D and E according to the likelihood and severity of harm and answer the section 5 about the measures, if you answered the question(s) with yes. If you answered every questions with no, you don't have to complete the section 5 and the DPIA tab III and can finish the DPIA with the consultation of the tab result.	**Answer**	**Risk rating - Likelihood** Rate the **possibility of the risk to occur** and choose between 1 to 3 whereas 1 means very low probability, 2 means medium probability and 3 means high probability.	**Risk rating - Severity** Rate the **extend of damage of the risk** between 1 to 3 whereas 1 means very low damage with low impact on the affected person, 2 means medium damage with probable impact on the affected person and 3 means high damage with high impact on the affected person.	**Risk rating result** **- scale:** **7 - 9 = high** **4 - 6 = medium** **1 - 3 = low** **0 = inapplicable**
4.1	Are individuals rated or assessed based on certain personal aspects? *(Evaluation or scoring)*	0			0
4.2	Does automated decision-making occur that could lead to the exclusion or disadvantages of persons? *(Automated-decision making with legal or similar significant effect)*	0			0
4.3	Are data subjects observed, monitored and controlled based on data collected via networks or on systematic monitoring of publicly accessible areas?	0			0
4.4	Are confidential and highly personal data or data that should be particularly worth protecting				

Figure 3 Screenshot from Version 1 – DPIA Questions

The final four tabs summarise the results and offer additional background (a terminology list, information about the artefact, and the bibliography).

Evaluation: The first version was evaluated with a demonstration and testing session during the 'Trinational Cybersecurity Days 2021' at the University of Applied Sciences and Arts Northwestern Switzerland FHNW (2021). The uncertainty of the test persons from small businesses about the high-risk categories and the risk rating implies that guidance and support is necessary because the procedure, language, and risk assessment in a DPIA require explanation. One essential feedback was that each of the tabs contained too much information at once; thus, the structure, content, and examples were perceived as too complicated, and the first version did not yet meet the goal of simplification for the target group. The received inputs were listed, analysed, and implemented into the next version.

DPIA Instrument Version 2: To improve the overall clarity, the second version is divided into 22 separate tabs – instead of just ten. For example, when conducting the actual DPIA, each question is positioned on an individual tab. Furthermore, navigation buttons and supporting comments were added. The structure and content still follow the concept of a DPIA mentioned in GDPR and related minimum requirements. Moreover, the tabs are labelled either with letters (to indicate informational content) or numbers (to indicate each step of the DPIA). Figure 4 shows a screenshot:

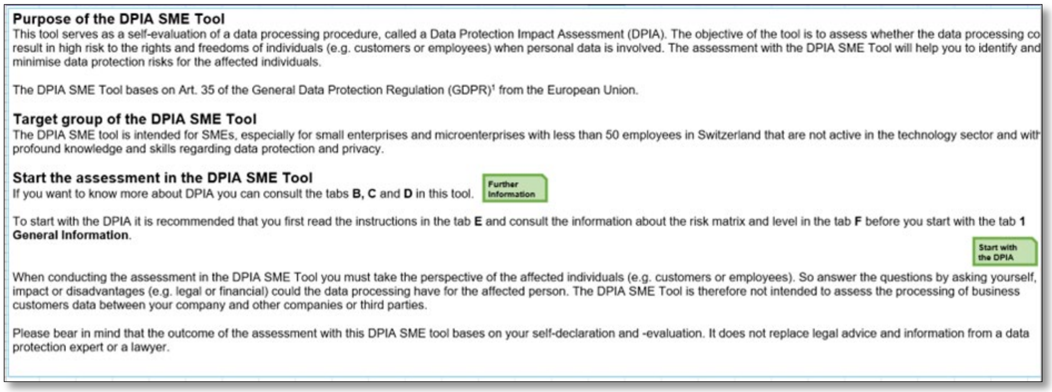


Data processing under review						
This section allows you to define and describe the scope of the processing in detail, to assess the risk, to define measures and indicate if the risk can be solved or mitigate with the measures.	**Answer**	**Justification of answer**	**Risk assessment**	**Measures planned to reduce the risk**	**Residual risk**	(Bayerisches Lande und Datenschutzau Commission Nationa l'Informatique et des 2018b; Datenschutz
Do you conduct automated decision making to help make decisions on someone's access to a service, opportunity or benefit? If your answer is Yes, please indicate which data processing example(s) is/are present in column D, rate the risk in Column E, describe the planned measures to reduce the risk for your customer and employees in column F and indicate the effect of the measures on the risk in column G.						
Perfect - you have answered the second part. Click on the button "Next" to continue.		***Examples of automated decision making are:***	***Indicate the level of risk***	***Define the measures that you plan to implement to reduce the risk for your customers and employees. Examples of measures are:***	***Indicate if the risk is eliminated, reduced or accepted with the planned measures.***	Next
		Exclusion criteria in an application procedure leading to an automated decision that results in the exclusion of a candidate, etc.	*Please consider that every data processing can have a possible negative impact on the affected individuals and result in risks for them. Nevertheless, the risks are usually low or medium and rarely high. High risks are present if the rights and freedom of the affected individuals could be severely*	***Inform the customer or employee about the automated-decision making and obtain consent from them for the data processing*** *by offering terms & conditions (either on paper or online) where you present the purpose and type of data to be processed, the user rights, confidential clause, information about the possibilities to access, download, erase and rectify personal data, privacy settings, possibility to excluse of the processing if*	*Please describe the effect of the planned measures on the risk by indicating if the risk is eliminated, reduced or accepted.*	

Figure 4 Screenshot from Version 2 – DPIA Questions

Evaluation: The second version was first evaluated during three testing sessions with representatives from the personas. Two of the small businesses have employees, and one is a one-person company. The evaluation took place in individual sessions and was enriched with a focus group session during a further education course at FHNW. The participants initially struggled to understand the aim of the DPIA; they understood the purpose better after the tests and realised the benefit of such an approach. As the testers could clarify uncertainty with the researcher, the independent self-evaluation with our instrument could not be examined. Nevertheless, conducting a DPIA and raising awareness among could be proven. Version 2 was furthermore tested by experts with a background in IT, law and information risk and security. The experts proposed that certain parts need to be implemented in addition or improved. The experts confirmed that the questions and tabs which were developed for this version cover the relevant high-risk categories when processing personal data. The overall result from the test was that the structure and content fulfilled the criteria of accuracy and completeness.

DPIA Instrument Version 3 - Excel: Based on the results and feedback described above, the third version was developed. To further reduce the complicacy, version 3 consists of 24 tabs, each covering only one topic or question. Because the navigation worked well in the second evaluation round, the splitting of the high-risk categories and questions in separated tabs were maintained. The final version follows the concept of a DPIA mentioned in GDPR and the minimum requirements. The main adjustment is the tab 'A Purpose and Target group' that provides information on the scope and target audience of the DPIA instrument (Figure 5) as these crucial points were unclear previously.



Purpose of the DPIA SME Tool

This tool serves as a self-evaluation of a data processing procedure, called a Data Protection Impact Assessment (DPIA). The objective of the tool is to assess whether the data processing co result in high risk to the rights and freedoms of individuals (e.g. customers or employees) when personal data is involved. The assessment with the DPIA SME Tool will help you to identify and minimise data protection risks for the affected individuals.

The DPIA SME Tool bases on Art. 35 of the General Data Protection Regulation (GDPR)[1] from the European Union.

Target group of the DPIA SME Tool

The DPIA SME tool is intended for SMEs, especially for small enterprises and microenterprises with less than 50 employees in Switzerland that are not active in the technology sector and with profound knowledge and skills regarding data protection and privacy.

Start the assessment in the DPIA SME Tool

If you want to know more about DPIA you can consult the tabs **B, C** and **D** in this tool.

To start with the DPIA it is recommended that you first read the instructions in the tab **E** and consult the information about the risk matrix and level in the tab **F** before you start with the tab **1 General Information**.

When conducting the assessment in the DPIA SME Tool you must take the perspective of the affected individuals (e.g. customers or employees). So answer the questions by asking yourself, impact or disadvantages (e.g. legal or financial) could the data processing have for the affected person. The DPIA SME Tool is therefore not intended to assess the processing of business customers data between your company and other companies or third parties.

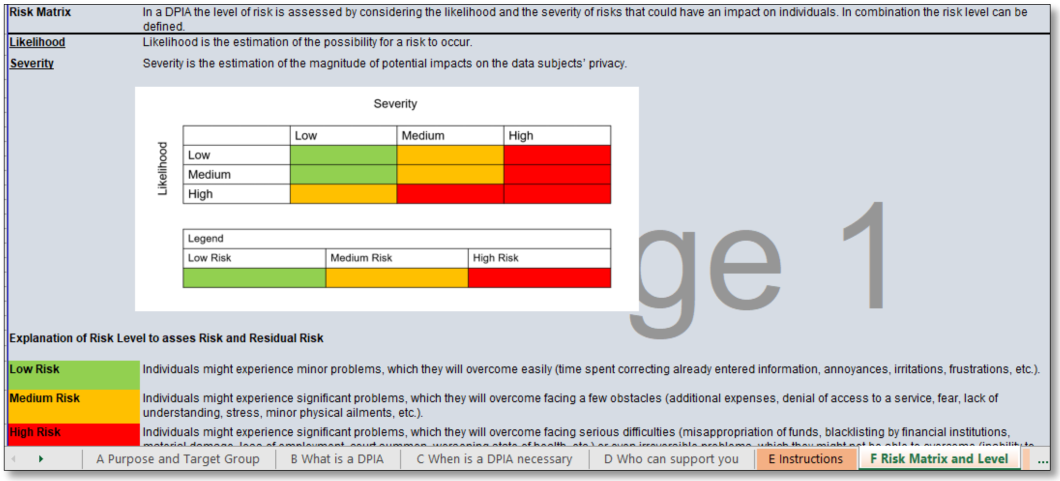
Please bear in mind that the outcome of the assessment with this DPIA SME tool bases on your self-declaration and -evaluation. It does not replace legal advice and information from a data protection expert or a lawyer.

Figure 5 Screenshot from Final Excel Version – Purpose and Target Group

Moreover, a new tab ´F Risk Matrix and Level´ including explanations about risk level and effects on risks to support the user in the risk and residual risk rating was added (Figure 6). The possibility to prove that a DPIA necessity check or a DPIA was conducted was added to two additional tabs (´2 Data Description Check´ and ´4 Result´). These tabs can be printed, signed, and securely stored as compliance proof.

In version 2, there was a lack of ability to specify the effect of the measures on the risk, so this feature was added to each tab containing questions about data processing. This effect on the risk can be specified using suggested values 'accepted', 'reduced', or 'eliminated'. The residual risk level may be specified as 'high', 'medium', or 'low' as these categories are more common to define risk level.

In the tabs 'G Overview Data Processing' and '4 Result', the achieved values are compared to threshold values for a high risk. The thresholds were determined based on the few identified criteria from literature and DPIA instruments under review. This comparison should help to improve interpretability. The final evaluation of the (residual) risk indicates high risk if a residual risk is rated as 'high' and the effect on the residual risk is rated as 'accepted' at least once. In addition to this criterion, a medium or high residual risk in the final residual risk evaluation is also incorporated to ensure that the outcome of the DPIA results more often in high risk – and hence to raise awareness.



Risk Matrix In a DPIA the level of risk is assessed by considering the likelihood and the severity of risks that could have an impact on individuals. In combination the risk level can be defined.

Likelihood Likelihood is the estimation of the possibility for a risk to occur.

Severity Severity is the estimation of the magnitude of potential impacts on the data subjects' privacy.

Severity

Likelihood	Low	Medium	High
Low	🟩	🟧	🟥
Medium	🟩	🟧	🟥
High	🟧	🟥	🟥

Legend		
Low Risk	Medium Risk	High Risk
🟩	🟧	🟥

Explanation of Risk Level to asses Risk and Residual Risk

Low Risk Individuals might experience minor problems, which they will overcome easily (time spent correcting already entered information, annoyances, irritations, frustrations, etc.).

Medium Risk Individuals might experience significant problems, which they will overcome facing a few obstacles (additional expenses, denial of access to a service, fear, lack of understanding, stress, minor physical ailments, etc.).

High Risk Individuals might experience significant problems, which they will overcome facing serious difficulties (misappropriation of funds, blacklisting by financial institutions,

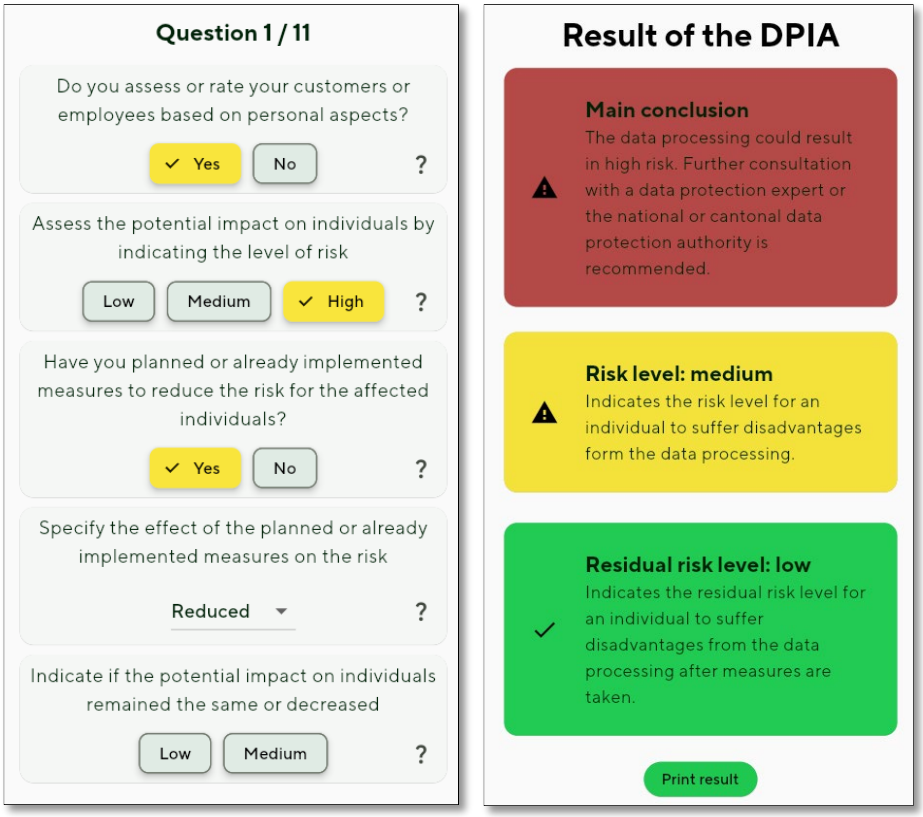
Figure 6 Screenshot from Final Excel Version – Risk Matrix and Level

Simplification could be reached by reducing the number of questions in the necessity checklist to three questions ('2 Data Description Check') and incorporating explanations and examples from diverse existing guidelines and instruments. The final DPIA instrument incorporates the concept of a DPIA mentioned in GDPR and related minimum requirements. The nine risk factor categories from the guidelines of the WP29 (2017) and the two additional risk factor categories mentioned in other guidelines and instruments (CNIL, 2021; Datenschutzstelle Fürstentum Liechtenstein, 2020; ICO, 2021) define the structure.

DPIA Instrument Version 3 – Application: While the Excel version is a good instrument to learn how DPIA works, it lacks a core element that should lay in the very basis of any instrument for non-experts – usability as well as data assurance, auditability respectively. This shortcoming evolved over time, as each evaluation led to enhancements at the cost of reduced simplicity. Moreover, using the instrument from a mobile device, e.g., phone or tablet, showed to be a rising desire when using the DPIA instrument operationally. Therefore, a cross-platform application with user-friendly interface that can be compiled for web, desktop and mobile devices was developed. This application is based on the Excel-based version 3 but makes the assessment quicker and easier – from a usability perspective.

The key feature of the application is a front-end based generation of a PDF file containing core information about the data processing inserted by the user. The application still satisfies data protection requirements. From a technological point of view, there is no interaction between application and any web server, so the information that a user provides is not stored persistently. Moreover, if the DPIA necessity check indicates that no DPIA is needed, the web-based application generates a simplified PDF file, which only contains proof of no need of conducting a DPIA. In both cases, a PDF file can be printed and signed by the responsible person, e.g., the business owner.

The web-based application still has a section for users who are new to DPIA and GDPR. It is based on the content from the Excel version, whereas some elements (e.g., risk matrix, risk level description) were moved to a hint system which is implemented directly into the DPIA process. Thus, users will move on from learning to risk assessment faster, and there is no need to switch the screen/tab; all answers to questions that may occur can be found immediately during the DPIA process only by pressing the button. The following figure represents screenshots from the web-based final version 3 of the DPIA.



Question 1 / 11

Do you assess or rate your customers or employees based on personal aspects?

[✓ Yes] No ?

Assess the potential impact on individuals by indicating the level of risk

Low Medium [✓ High] ?

Have you planned or already implemented measures to reduce the risk for the affected individuals?

[✓ Yes] No ?

Specify the effect of the planned or already implemented measures on the risk

Reduced ▾ ?

Indicate if the potential impact on individuals remained the same or decreased

Low Medium ?

Result of the DPIA

⚠ **Main conclusion**
The data processing could result in high risk. Further consultation with a data protection expert or the national or cantonal data protection authority is recommended.

⚠ **Risk level: medium**
Indicates the risk level for an individual to suffer disadvantages form the data processing.

✓ **Residual risk level: low**
Indicates the residual risk level for an individual to suffer disadvantages from the data processing after measures are taken.

Figure 7 Screenshots from final Web Version of the persona-oriented DPIA for Small Businesses

Usability was the key to the whole development approach. Hence, fields where users can justify some answers were omitted to keep the procedure fast and to make the interface more lightweight. For those data processing categories which can cause medium or high risk there is however a possibility to justify the answers and further steps in the generated PDF printout. The web-based version 3 is designed in a way allowing to adjust contents and process steps to fit the requirements of any data processing law if needed in future.

Evaluation: Version 3 was tested during a further education seminar at FHNW with small business representatives. Participants recognised the simplicity of the instrument and the high usability. Some participants mentioned that in comparison with the Excel version they miss the opportunity to enter context information, e.g., justifications for answers and explanations of concrete measures to address each risk. There were some concerns that the PDF does not store enough information to guarantee the data assurance or auditability and it would be difficult to understand the result when they will reconsult the document after a few weeks/months. One participant mentioned that the PDF should be offered in a format that would allow entering free text so that no Adobe license would be necessary to add text and information. This means that there are useful improvements to the current solution that at the same time will be easy to use and will provide a more detailed DPIA.

4 Conclusion

To sum up, our research applied DSR and led to a persona-oriented DPIA instrument addressing the special situation of non-technology small businesses and their owners. Personas were identified through literature review and interviews with representatives that drove the development and helped through multiple evaluations to prove that our result is compliant with the minimal requirements defined in the GDPR. One ongoing challenge we faced throughout the research process was to balance simplification with comprehensiveness which is necessary to fulfill GDPR compliance requirements. Every evaluation phase led to valid enhancements for improving interpretability that reduced the speed and ease of conducting the DPIA. As mitigation, we decided to produce two operational artefacts – one Excel-based and one web-based variant. The software-based instrument could serve as the low-threshold entry point for non-experts to start with DPIA. It offers a simple and fast first experience when conducting DPIAs and aims at raising data protection awareness. Once more elaborated DPIA processes are desired or for users that desire more background information, the Excel-based instrument would offer more comprehensiveness and control of the steps.

Our two artefacts provide a benefit both for academia and practice. The target group on non-technology small businesses is offered a choice of two low-threshold DPIA instruments adapted to a tight resource situation and fitting to a non-expert knowledge level. The DPIA instruments – Excel and web-based application – are used operationally in (further) education at FHNW. In the further education programs, many of the participants match our selected personas. For the Excel-variant, a sample fitting to each of the personas is publicly available for practical guidance [2].

From an academic perspective, our research has contributed to addressing an existing gap – assisting non-experts in small businesses to comply with GDPR. With this paper and by publishing both artefacts free to use and adapt under an open-source license [3], we aim to enrich the academic discourse and provide opportunities for future research.

References

Barnard-Wills, D., Cochrance, L., & Marchetti, F. (2019). Report on the SME experience of the GDPR (Deliverable D2.2 (Version 1.0)). STAR Consortium. https://www.trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf

Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In S. Schiffner, J. Serna, D. Ikonomou, & K. Rannenberg (Eds.), Privacy Technologies and Policy (Vol. 9857, pp. 21–37). Cham: Springer. https://doi.org/10.1007/978-3-319-44760-5_2

Bieker, F., Martin, N., Friedewald, M., & Hansen, M. (2018). Data Protection Impact Assessment: A Hands-On Tour of the GDPR's Most Practical Tool. In M. Hansen, E. Kosta, I. Nai-Fovino, & S. Fischer-Hübner (Eds.), Privacy and Identity Management. The Smart Revolution (Vol. 526, pp. 207–220). Cham: Springer. https://doi.org/10.1007/978-3-319-92925-5_13

CNIL (2021). PIA software. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

Dashti, S., & Ranise, S. (2020). Tool-Assisted Risk Analysis for Data Protection Impact Assessment. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, & S. Fricker (Eds.), Privacy and Identity Management. Data for Better Living: AI and Privacy (Vol. 576, pp. 308–324). Cham: Springer. https://doi.org/10.1007/978-3-030-42504-3

[2] https://drive.switch.ch/index.php/s/GP5Q5d42YWnRfzV

[3] Link to DPIA Instrument – Web-based: https://digitaltrust.pages.fhnw.ch/dpia-tool/#/;
Link to DPIA Instrument – Excel-based: https://drive.switch.ch/index.php/f/5982503971

Datenschutzstelle Fürstentum Liechtenstein (2020). Datenschutz-Folgenabschätzung Schwellwertanalyse (v1.0). www.datenschutzstelle.li/download_file/542/328

European Commission. (2020). Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition. Two years of application of the General Data Protection Regulation (SWD(2020) 115 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

GDPR, Legislation Regulation (EU) 2016/679, (EU) 2016/679 (2018). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Grütter, B., & Schneider, B. (2019). Data protection impact assessment guidelines in the context of the general data protection regulation. In Thriving on Future Education, Industry, Business and Society; Proceedings of the MakeLearn and TIIM International Conference (pp. 261-270). ToKnowPress.

Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems (Vol. 28). Boston, MA: Springer. https://doi.org/10.1007/978-1-4419-5653-8

ICO (2018). How do we do a DPIA? Sample DPIA Template 20180622 v0.4. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how2

ICO (2021). Codes of conduct. https://ico.org.uk/for-organisations/
guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/codes-of-conduct/

Junior, P. T. A., & Filgueiras, L. V. L. (2005). User modeling with personas. Proceedings of the 2005 Latin American Conference on Human-Computer Interaction - CLIHC '05, 277–282. https://doi.org/10.1145/1111360.1111388

Levy, Y., & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing Science: The International Journal of an Emerging Transdiscipline, 9, 181–212. https://doi.org/10.28945/479

Office of the Information and Data Protection Commissioner Malta (2020). Guidelines on DPIA template. https://idpc.org.mt/wp-content/uploads/2020/07/Guidelines-on-DPIA-template.pdf

Trinational cybersecurity days. (2021, April 1). Retrieved from https://www.tri-csd.ch/trinational-cybersecurity-days-2021/

Vaishnavi, V. K., & Kuechler, W. (2015). Design Science Research Methods and Patterns: Innovating Information and Communication Technology (2nd Edition). Boca Raton: CRC Press. https://doi.org/10.1201/b18448

Vemou, K., & Karyda, M. (2019). Evaluating privacy impact assessment methods: Guidelines and best practice. Information & Computer Security, 28(1), 35–53. https://doi.org/10.1108/ICS-04-2019-0047

WP29 (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Wright, D., Finn, R., & Rodrigues, R. (2013). A Comparative Analysis of Privacy Impact Assessment in Six Countries. Journal of Contemporary European Research, 9(1), 160–180.