PIAs in the Wild: Scoping Review – Positive and Negative Aspects

Summary of themes and sub-themes with associated references

Name	Examples	Files	References
Negative Aspects - Barriers, challenges, hindrances, disadvantages	**Main barriers, challenges, and hindrances for PIAs as reported in practice.**	39	Ahmadian et al. (2018) Alaqra et al. (2021) Alaqra et al. (2023) Bamberger and Mulligan (2012) Bas Seyyar and Geradts (2020) Bayley and Bennet (2012) Brautigam (2012) Clarke (2016) Dashti et al. (2021) Deadman and Chandler (2012) Easton (2017) Edwards (2012) Ferra et al. (2020) Friedewald et al. (2022) Henriksen-Bulmer et al. (2020) Horák et al. (2019) Iwaya et al. (2019) Iwaya et al. (2023) Kroener et al. (2021) McKee (2022)

Name	Examples	Files	References
			Nas (2019) Parks et al. (2011) Rehak et al. (2022) Schneider et al. (2023) Sharma and Kaushik (2017) Shin et al. (2017) Stewart (2012) Stoddart (2012) Thoma (2012) Todde et al. (2020) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2020) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012)
01 - Methodological Weaknesses	**Inherent Challenges of Risk Assessment** “A factor somewhat overlooked at this stage was the fact that the project pursues innovation and that this creates shifting ground for the PIA in the sense that it is not clear what kinds of technologies and what kinds of uses will be developed, or even the specific goals the innovation aims to achieve.” (Easton, 2017)	26	Ahmadian et al. (2018) Alaqra et al. (2021) Alaqra et al. (2023) Bamberger and Mulligan (2012) Bas Seyyar and Geradts (2020) Bayley and Bennet (2012)

Name	Examples	Files	References
	PIA methodologies need to be streamlined or are too complicated and complex “Industry experts that evaluated this model thought the model was attempting to do too much. While they liked the idea of addressing risk, this model intermingled privacy assessment steps with risk management and was no longer simple and easy to follow.” (McKee, 2022) “Many respondents felt that the PIA Handbook is ‘not business friendly’, that it was ‘too onerous and detailed’, ‘too high level’, ‘too dense and complex’, or ‘too general’ to serve the company’s objectives.” (Wright et al. , 2014) **Low credibility or proven effectiveness of PIA-related methods** “While methodologies for PIAs continue to emerge, there has been limited evidence to date to indicate how effective PIAs really are in attaining their stated goals.” (Wadhwa, 2012) **Subjectivity** “The organisations that used privacy advisors mentioned that the quality of the determined the privacy risks was very dependent on the skills and experience of the person determining that risk. The data protection officers who were interviewed perceive the process of deriving privacy risks based on the filled-out questionnaire as vague.” (Van Puijenbroek and Hoepman, 2017)		Brautigam (2012) Easton (2017) Edwards (2012) Ferra et al. (2020) Friedewald et al. (2022) Iwaya et al. (2019) McKee (2022) Nas (2019) Schneider et al. (2023) Sharma and Kaushik (2017) Stewart (2012) Stoddart (2012) Thoma (2012) Todde et al. (2020) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Wright et al. (2014) Wrigth and De Hert (2012)
02 - Bad Practices and	**Inconsistent Conduction of PIAs**	19	Bayley and Bennet (2012) Brautigam (2012)

Name	Examples	Files	References
Poorly Conducted PIAs	"[…] privacy impact assessments were carried out in an inconsistent manner – for example, some privacy officers had some involvement in their organisation's development of new product and services, whilst others were involved in reviewing suppliers to ensure that the proper contractual controls were in place. However, there was no clear means of measuring when and where privacy impact assessments were carried out, whether the outputs were of a consistent quality and resulted in effective change." (Deadman and Chandler, 2012) **Insufficient Information for Doing a PIA** "The main factor that slows execution of assessments is lacking documentation in the project. This is in particular the case with legacy cases or when third parties are involved. Sometimes, incomplete information is passed on when projects move from research and development units to the business units." (Brautigam, 2012) **Inappropriate Risk Analysis** "On the one hand risks are overlooked which emerge from scenarios beyond normal processing activities: the (rare) cases in which law enforcement and supervisory authorities gain access to data are also often not problematized. On the other hand, there is often still a lack of awareness that the greatest risks usually come from processing for the intended purposes and by authorised actors […]" (Friedewald et al. , 2022) **Disregard for Data Subjects** "We also found that while organisations are comfortable assessing risks from an organisational perspective, they		Clarke (2016) Deadman and Chandler (2012) Ferra et al. (2020) Friedewald et al. (2022) Henriksen-Bulmer et al. (2020) McKee (2022) Rehak et al. (2022) Shin et al. (2017) Stewart (2012) Stoddart (2012) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wright et al. (2014) Wrigth and De Hert (2012)

Name	Examples	Files	References
	struggled to appreciate that the DPIA requires them to consider risks from the perspective of their customers or service recipients and what this means in practice" (Henriksen-Bulmer et al. , 2020)		
03 - Perfunctory PIAs	**Ceremonial or pro forma performance of PIAs** "However, the tension between agency mission and external mandates can result in the "ceremonial" performance of mandated processes, whereby an organisation adapts external mandates in ways that most easily achieve the appearance of legitimacy, while minimising the dislocation of existing practices and priorities." (Bamberger and Mulligan, 2012) **PIA is conducted ex post facto or when it is already too late and changes are limited and costly** "We found that PIAs were viewed as a regulatory obligation independent of an entity's program responsibilities, rather than the sort of specialised and integrated risk management tool they were designed to be. […] the government institutions we audited generally viewed PIAs as an administrative burden, to be completed *ex post facto*, rather than in the planning stages of new program and service deliveries." (Stoddart, 2012)	15	Bamberger and Mulligan (2012) Bayley and Bennet (2012) Clarke (2016) Dashti et al. (2021) Easton (2017) Edwards (2012) Ferra et al. (2020) McKee (2022) Stoddart (2012) Thoma (2012) Van Puijenbroek and Hoepman (2017) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wrigth and De Hert (2012)
04 - Lack of Organisational Processes for PIAs	**Lack of management support and infrastructure for PIAs** "A present limitation is that threats and risks are not standardized or categorized and that the organizational process of managing such methodology was not defined yet. More specifically, in the long term, there should be a	14	Bamberger and Mulligan (2012) Bayley and Bennet (2012) Brautigam (2012) Iwaya et al. (2023) McKee (2022)

Name	Examples	Files	References
	specific actor within the hospital organization in charge of maintaining and updating the documentation related to the DPIA and produced using the proposed methodology." (Todde et al. , 2020) **PIAs are not being carried out** "Ovewhelming majority of attendees, nearly 75%, responded they do not currently conduct holistic privacy assessments as part of their organizational, security or privacy assessment processes." (McKee, 2022) **Lack of internal audit evaluation processes** "Little or no auditing of the privacy impact assessment was performed." (Van Puijenbroek and Hoepman, 2017)		Shin et al. (2017) Stoddart (2012) Thoma (2012) Todde et al. (2020) Van Puijenbroek and Hoepman (2017) Wadhwa (2012) Warren and Charlesworth (2012) Wright et al. (2014) Wrigth and De Hert (2012)
05 - Lack of Privacy-Related Knowledge	**Confusing privacy with security and confidentiality** "Failing to recognize the boundaries between security and privacy can result in misjudging either the necessity of the DPIA or the impact level of data processing on data subjects." (Dashti, 2021) **Clearly explain and set expectations to clients, regulators and others the PIA process and deliveries** "The principal challenge this author has found is different assumptions among clients, regulators and others as to what the assessment process is intended to do and is capable of delivering. The key to maintaining the integrity and credibility of the process is to ensure that the client is fully informed as to the options, and the implications of each of his or her choices." (Edwards, 2012)	14	Bayley and Bennet (2012) Brautigam (2012) Dashti et al. (2021) Edwards (2012) Friedewald et al. (2022) Nas (2019) Rehak et al. (2022) Schneider et al. (2023) Stewart (2012) Stoddart (2012) Thoma (2012) Todde et al. (2020) Wright et al. (2014) Wrigth and De Hert (2012)

Name	Examples	Files	References
	Confusion or uncertainty about the roles of data processors and joint data controllers “Another issue that is common amongst many global Internet and Software as a Service providers, is the uncertainty about their role as data processors (Article 4(7) GDPR[22]) or (joint) data controllers (Articles 4(8) and 26 GDPR[23]).” (Nas, 2019)		
06 - Organisation's Lack of Resources for PIAs	**Lack of PIA expertise or experts** “Perhaps the greatest difficulty encountered by the ONS was in locating appropriate expertise on PIAs.” […] Yet, although the ONS found the PIA handbook to be helpful, especially in outlining the processes to be enacted and requiring it to check legal compliance, it was unable to make contact with anyone with direct experience of conducting PIAs in the UK.” (Warren and Charlesworth, 2012) **Lack of resources for conducting PIAs** “We have seen many situations where some project teams’ initial reluctance to work with us in documenting and assessing privacy aspects (typical arguments were missing resources, expected delays, additional cost, lack of need) changed completely within a short time.” (Thoma, 2012) **PIAs are seen as a burden or a hurdle** “The Lithuanian and Dutch DPAs said that it is better when government agencies and private sector companies have their PIAs audited by an independent third party, but they didn’t think that it should be mandatory, because it could	13	Bayley and Bennet (2012) Brautigam (2012) Edwards (2012) Ferra et al. (2020) Friedewald et al. (2022) Stoddart (2012) Thoma (2012) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012)

Name	Examples	Files	References
	be too big a financial burden for those companies and agencies that don't have enough financial capacity for this or could lead to unnecessary costs." (Wright and Wadhwa, 2013)		
07 - Poor Stakeholder Consultation	**Lack of mechanisms for public participation or consultation** "Further, the lack of explicit mechanisms for public participation in the PIA process limits the opportunities for outside experts to assist the agency in identifying the privacy implications of often complex technological systems." (Bamberger and Mulligan, 2012) **Public participation is obstructed or suggestions are ignored** "[…] participation by the public and by advocacy organisations has been precluded, or limited to submissions at a very late stage in the project – almost always only after legislation has been drafted and tabled; […]" (Clarke, 2016)	13	Bamberger and Mulligan (2012) Bayley and Bennet (2012) Clarke (2016) Easton (2017) Friedewald et al. (2022) Kroener et al. (2021) Rehak et al. (2022) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wrigth and De Hert (2012)
08 - Poor Public Reporting of PIAs	**PIAs are not made available to the public** "PIA reports are inconsistently accessible, whether because they are not published at all, or essentially hidden by posting them on agency websites without obvious links. For private sector organizations, published PIAs are nearly non-existent." (Wadhwa. 2012) **Fears and barriers to releasing a public PIA** "A challenge for SecInCoRe, which by its very nature included treatment of sensitive data, was to determine the	13	Bamberger and Mulligan (2012) Bayley and Bennet (2012) Clarke (2016) Easton (2017) Edwards (2012) Iwaya et al. (2023) Rehak et al. (2022) Van Puijenbroek and Hoepman (2017) Wadhwa (2012)

Name	Examples	Files	References
	extent to which the PIA and related reporting can be made public. It felt within the project that making the process public could significantly change the PIA, making participants far more guarded, obstructing self-criticism." (Easton, 2017)		Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013) Wrigth and De Hert (2012)
09 - Competing Priorities	**PIAs can incur extra costs and delays** "The Luxembourg DPA said PIAs could involve extra costs and time, especially for start-ups, small, and medium-sized companies." (Wright and Wadhwa, 2013) **PIAs may disrupt the internal workings of an organisation** "The idea that the central functions of the service are to be kept and that the data protection considerations should not unnecessarily impede business goals is a recurring thought." (Vandercruysse et al, 2021)	12	Alaqra et al. (2021) Bamberger and Mulligan (2012) Bayley and Bennet (2012) Parks et al. (2011) Stewart (2012) Thoma (2012) Todde et al. (2020) Vandercruysse et al. (2020) Vandercruysse et al. (2021) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012)
10 - Lack of Regulator's Processes and Guidance	**Lack of mechanisms in the government for accountability of the implementation of the PIAs plans, promised mitigation measures** "Currently, there is no reporting mechanism in Canada for the implementation of PIA plans, except in the rare instance where the process of review yields instructions to organisations to provide the actual mitigation measures. " (Bayley and Bennet, 2012) **There is no central registry of PIA reports**	10	Bayley and Bennet (2012) Edwards (2012) Shin et al. (2017) Stewart (2012) Van Puijenbroek and Hoepman (2017) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013)

Name	Examples	Files	References
	“How many privacy impact assessments this has resulted in is impossible to know. [...] There is no central register of PIA reports, and no requirement that they be shared with the Privacy Commissioner or published anywhere.” (Edwards, 2012)		Wright et al. (2014) Wrigth and De Hert (2012)
11 - Regulator's Lack of Resources for PIAs	**Lack of resources for PIA-related activities on the regulators' side** “Back in the privacy world, the practical reality is that privacy regulators will never be given the resources to carry out a “second assessment” (or audit) of every PIA, and are unlikely even to be able to adequately supervise private sector assessors who are engaged directly by project proponents.” (Waters, 2012) **Undermining the regulatory agencies** “However, after its election in late 2013, the new Government deliberately emasculated the Privacy Commissioner’s host organisation, the Office of the Australian Information Commissioner (OAIC), by denying funding to it.” (Clarke, 2016)	7	Bayley and Bennet (2012) Clarke (2016) Stewart (2012) Thoma (2012) Waters (2012) Wright and Wadhwa (2013) Wrigth and De Hert (2012)
12 - Lack of Regulatory Requirements	**PIAs were not mandatory for the public or private sector** “Due to these limitations, there are no requirements in Germany to always conduct PIAs for IT systems [...]” (Thoma, 2012) “[...] the problem with implementing PIA is the lack of clear regulation, preferably in a legal act, and of unified form and method. Until the PIA is explicitly seen as an obligation, its conduct relies on the controller’s good will	7	Bayley and Bennet (2012) Clarke (2016) Shin et al. (2017) Stoddart (2012) Thoma (2012) Wright and Wadhwa (2013) Wrigth and De Hert (2012)

Name	Examples	Files	References
	which is not always present especially when it comes to personal data processing and protection of the privacy rights." (Wright and Wadhwa, 2013)		
13 - Implementation Challenges Post-PIA	**The challenge to implement the identified measures after a PIA is completed** "Nokia has learned that having the findings alone is not enough; the key is to have a supporting structure that follows up on the status of those findings. This sounds obvious; however, implementation requires different people with different roles in the company to be aware of the findings. Almost all persons interviewed for this chapter saw implementation of reported findings as one of the core challenges." (Brautigam, 2012) **PIAs do not bring about actual change in organisational practices** "[…] the client did not welcome many of the recommendations, and there was considerable tension during the finalisation of the report, leading to a final product which did not highlight key recommendations, leaving them to be "discovered" by readers in the body of a lengthy document. As predicted in the general discussion above, this unsurprisingly meant that the PIA work was not used as effectively by potential critics [...]" (Waters, 2012)	6	Bamberger and Mulligan (2012) Brautigam (2012) McKee (2022) Stoddart (2012) Waters (2012) Wrigth and De Hert (2012)
14 - Conflict of Interests	**Conflict of interest of internal or external independent assessors** "However, if the independence of in-house staff can be impugned by regulators or opponents of a particular	5	Edwards (2012) Friedewald et al. (2022) Warren and Charlesworth (2012) Waters (2012)

Name	Examples	Files	References
	project, why should a consultant, whose livelihood and reputation depend on delivering work which pleases, rather than annoys those who pay him or her, have any extra credibility?" (Edwards, 2012) "Finally most participants are employees of an organisation or company and therefore have to act in accordance with what is in the best interests of the business. This can lead to tensions when they are supposed to assess risks in an unbiased way from the point of view of the people concerned." (Friedewald et al, 2022)		Wrigth and De Hert (2012)
15 - Political Barriers to PIAs	**Political barrier - privacy vs national security** "Expending political capital on privacy can be risky. While polls consistently reveal deep concern about information abuse and support for privacy protections in general[30], individual decisions frequently counterpose privacy against two other powerful values: efficiency and security." (Bamberger and Mulligan, 2012) **Political barrier - conflicts of PIAs and policy-making** "The reasons for poor consideration of privacy risks in the policy-making process vary from the 'complexity of the policy-making picture', involving several ministers and bargaining consultations, to the need 'to get on' with policy making and delivery of the final outcome." (Wright et al, 2014)	5	Bamberger and Mulligan (2012) Clarke (2016) Horák et al. (2019) Wright et al. (2014) Wrigth and De Hert (2012)
16 -	**Lack of interest from stakeholders in participating**	3	Warren and Charlesworth

Name	Examples	Files	References
Stakeholders' Lack of Interest in Privacy	**in the consultation process** "In addition, the ONS expressed disappointment with the response to its stakeholder consultation. In spite of receiving a list of civil society organisations from the ICO, and issuing direct invitations to these and related bodies, representatives from only two groups attended the consultation event (with another individual contributing via e-mail) and neither provided particularly meaningful feedback." (Warren and Charlesworth, 2012)		(2012) Wright and Wadhwa (2013) Wrigth and De Hert (2012)
Positive Aspects - Enablers, opportunities, drivers, advantages	**Main enablers, opportunities, and advantages of PIAs as reported in practice.**	43	Alaqra et al. (2021) Alaqra et al. (2023) Bamberger and Mulligan (2012) Bas Seyyar and Geradts (2020) Bayley and Bennet (2012) Brautigam (2012) Campanile et al. (2022) Clarke (2016) Dashti et al. (2021) Deadman and Chandler (2012) Di Iorio et al. (2009) Easton (2017) Edwards (2012) Ferra et al. (2020) Friedewald et al. (2022) Henriksen-Bulmer et al. (2020) Horák et al. (2019) Iwaya et al. (2019)

Name	Examples	Files	References
			Iwaya et al. (2023) Kroener et al. (2021) McKee (2022) Nas (2019) Parks et al. (2011) Pribadi and Suryanegara (2017) Rajamäki (2021) Rehak and Kuhne (2022) Rehak et al. (2022) Schneider et al. (2023) Sharma and Kaushik (2017) Shin et al. (2017) Stewart (2012) Stoddart (2012) Thoma (2012) Todde et al. (2020) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012) Zamorano et al. (2023)
01 - Ethics, Legal	**PIAs for meeting regulatory compliance** “These findings indicate that at the time of process set up	31	Bayley and Bennet (2012) Campanile et al. (2022)

Name	Examples	Files	References
Compliance, Communication with Regulators	at the offshore location, there is a strong focus on complying to the regulatory requirements as outlined in the privacy principles. This strategy is achieved with the help of the privacy program, collective involvement of the onshore and offshore teams and PIA." (Sharma and Kaushik, 2017) **Meeting legal and ethical obligations** "Privacy impact assessments require the judgement of competent privacy professionals using clear principles and an established risk assessment methodology to ensure Vodafone is able to pursue its commercial strategy while satisfying people's expectations regarding their privacy and meeting its legal and ethical obligations." (Deadman and Chandler, 2012) **PIAs as an accountability mechanism in the review or audit of implemented mitigation measures** "PIAs can act as an accountability mechanism when their review results in a requirement to submit specific mitigation tools as they are completed and as a starting point in complaint-driven or self-initiated investigations by a privacy commissioner." (Bayley and Bennet, 2012) **PIAs for demonstrating compliance with regulators** "DPIA not only allowed us to analyze the life cycle of the personal data in the platform and identify possible weak spots but also serves as an effective tool to demonstrate compliance to the data subjects, data protection authorities and also users of the platform." (Horák et al, 2019)		Deadman and Chandler (2012) Di Iorio et al. (2009) Easton (2017) Edwards (2012) Friedewald et al. (2022) Horák et al. (2019) Iwaya et al. (2019) Iwaya et al. (2023) Kroener et al. (2021) McKee (2022) Nas (2019) Parks et al. (2011) Pribadi and Suryanegara (2017) Rehak and Kuhne (2022) Rehak et al. (2022) Schneider et al. (2023) Sharma and Kaushik (2017) Shin et al. (2017) Stewart (2012) Stoddart (2012) Thoma (2012) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa

Name	Examples	Files	References
	PIAs as a basis for discussion with regulators "Proper DPIAs can help to enable and improve such discourses in a pluralistic and democratic society. Therefore DPIAs should generally be published so that they can be discussed not only by data protection regulators, but also by researchers, journalists, civil society and the general public" (Rehak and Kuhne, 2022)		(2013) Wright et al. (2014) Wrigth and De Hert (2012)
02 - Other Best Practices and Recommendations	**PIAs as Living Document** "It is worth noting that PIAs should be carried out before the development of such platforms. Whenever a shift in privacy objectives takes place during the design phase, LEAs should repeat the PIA to address new privacy risks." (Bas Seyyar and Geradts, 2020) "PIAs should be periodically reviewed, whenever assumptions change or when new threats are unveiled." (Iwaya et al, 2019) **Start Early to Maximise Results** "We therefore designed a workflow for the risk assessment of an information system establishing that the DPIA shall be performed after the purchase, usually a bid with strict IT security requirements of the information system, but before its deployment in the real environment." (Todde et al, 2020) "Because the PIA was commissioned at a very early stage in the consideration of options, and because the project team were committed to addressing privacy issues, both the initial report in December 2003 and a subsequent update report in April 2004 had significant influence on	28	Bamberger and Mulligan (2012) Bas Seyyar and Geradts (2020) Bayley and Bennet (2012) Brautigam (2012) Dashti et al. (2021) Deadman and Chandler (2012) Easton (2017) Edwards (2012) Ferra et al. (2020) Friedewald et al. (2022) Iwaya et al. (2019) Kroener et al. (2021) McKee (2022) Nas (2019) Rehak et al. (2022) Sharma and Kaushik (2017) Stewart (2012) Stoddart (2012) Thoma (2012) Todde et al. (2020)

Name	Examples	Files	References
	the choice of approach […] In this case, warnings in the PIA about the privacy risks inherent in the more ambitious options appear to have resulted in much more focussed, and less privacy intrusive, programs." (Waters, 2012) **Define the Scope of Analysis and Limitations** "PIAs were generally perceived to be more effective when […] their scope and depth are sensitive to a number of crucial variables: the size of the organisation, the sensitivity of the personal data, the forms of risk, the intrusiveness of the technology;" (Warren and Charlesworth, 2012) "What is most important for the assessor is to ensure that the scope constraints are clearly identified in the report, and that the report notes that it is based on that description. This protects the assessor when scope creep (or function creep or mission creep) infects the system or organisation […]" (Edwards, 2012) **Independence of privacy experts and assessors** "Clearly regulators have a useful role in this context as experts at arm's length from the proponents of a particular project. They represent the public interest and are expected to ensure that the process protects the public." (Stewart, 2012) "The representatives of each risk-managing function then prepare their assessments, which highlight any challenges and legal limitations and discuss the involved risks. It is vital that these assessments are independent, i.e., a negative data protection assessment cannot be overturned by an exceedingly positive statement from the		Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012)

Name	Examples	Files	References
	representative of another function. The assessments and recommendations – which can be anywhere between “no significant risks, proceed as proposed” or “project cannot be realised for legal reasons” – are made available to the initiators who are then expected to report back on how they intend to proceed. Frequently, this assessment is the starting point for a close co-operation between the project and the data protection organisation over the full project lifetime.” (Thoma, 2012) **Develop a Strong Process for PIAs** “Data protection consultants are primarily concerned with ‘sensible’ efficiency. More particularly with regard to the DPIA, scoping and project management are vital to handling the DPIA process efficiently.” (Vandercruysse et al, 2021) **Reuse and Make Available Past PIAs, Tools and Catalogues** “Those conducting large numbers of PIAs have been able to compile privacy risk and control/mitigation matrices to improve the efficiency with which PIAs may be completed as well as the quality of the PIA product. With this approach, knowledge is accumulated and passed on within an entity or from consultant to client in a cost-effective manner.” (Bayley and Bennet, 2012) “For many controllers, the immediate question arose as to how a risk could best be addressed. At this point, well-maintained catalogs of reference measures are of great benefit. Fortunately, such catalogs have already been created by national supervisory authorities [...]”		

Name	Examples	Files	References
	(Friedewald et al, 2022)		
03 - Protecting Individuals from Privacy Harms and Risk Reduction	**PIAs for better privacy, minimising privacy harms by identifying threats and appropriate controls** “The CNIL-PIA methodology on privacy risk assessment, and the related tool PIA, has been used to show the impact of those techniques and to show which could be the better way to obtain GDPR compliance in personal data used by learning machine tools to perform technical activities.” (Campanile et al, 2022) “Whilst we could find legitimate justifications—e.g., the use of consent—we came to the conclusion that the benefits did not justify the risks. […] The consortium therefore decided that collecting health data, and then defining and interpreting change progress metrics with regard to monitoring health, was too costly and too risky to justify the benefits, which could also be established through different means.” (Kroener et al, 2021) “Our PIA helps to bridge this gap by exposing the problems and providing controls (see Multimedia Appendix 4). On the basis of this PIA, engineers have a clearer path toward solving the privacy issues and ideally being able to address them at the very early stages of the design process, when changes are often simpler and less costly.” (Iwaya et al, 2019)	28	Alaqra et al. (2021) Alaqra et al. (2023) Bas Seyyar and Geradts (2020) Bayley and Bennet (2012) Campanile et al. (2022) Clarke (2016) Deadman and Chandler (2012) Edwards (2012) Henriksen-Bulmer et al. (2020) Horák et al. (2019) Iwaya et al. (2019) Iwaya et al. (2023) Kroener et al. (2021) Nas (2019) Rehak and Kuhne (2022) Rehak et al. (2022) Sharma and Kaushik (2017) Thoma (2012) Todde et al. (2020) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012)

Name	Examples	Files	References
			Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012) Zamorano et al. (2023)
04 - Stakeholder Consultation and Engagement	**Internal - Senior and Privacy Experts** “In particular, Kelly [i.e., the CPO leading the PIAs] assembled a staff of demonstrated privacy professionals with diverse disciplinary skills and not only located these employees in the central DHS privacy office, but embedded them within operational units throughout the agency. This combination of privacy expertise, varied training and perspective, and decentralised integration throughout decision-making structures, was particularly well suited to take advantage of the privacy impact assessment mechanism, an inherently interdisciplinary tool for affecting decision-making from the "bottom up".” (Bamberger and Mulligan, 2012) **Internal - Collaboration Cross-Teams and with Domain Experts** “This case study reveals that threats in police sector that can lead to privacy risks are rather different from those in other sectors. Collaboration between the investigators and PIA practitioners is crucial in precisely specifying these threats. The implementation of a PIA encourages privacy awareness within the investigators and the developers of a big data forensic platform.” (Bas Seyar and Geradts, 2020) **Internal - Management Support** “To foster integration of privacy impact assessment and	26	Alaqra et al. (2021) Bamberger and Mulligan (2012) Bas Seyyar and Geradts (2020) Bayley and Bennet (2012) Brautigam (2012) Dashti et al. (2021) Deadman and Chandler (2012) Easton (2017) Edwards (2012) Friedewald et al. (2022) Henriksen-Bulmer et al. (2020) Rehak et al. (2022) Schneider et al. (2023) Sharma and Kaushik (2017) Stewart (2012) Stoddart (2012) Thoma (2012) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth

Name	Examples	Files	References
	risk and project management, more actions need to be taken. Several said it was important to gain buy-in from senior management and develop privacy awareness and culture within the company, sustained by effective communication and training." (Wright et al, 2014) **Internal - Engage Project Members** "Furthermore, there was the need to ensure that partners did not see the PIA as a constraining exercise which just needed to be completed to placate the legal team. To achieve this, the presentation focused on the wider benefits of the PIA in relation to transparency, confidence and the streamlining of processes which could be beneficial to the project itself and to the partner organizations." (Easton, 2017) **External - Engaging external stakeholders for better PIAs** "A significant part of addressing many of these more strategic issues is the need for engagement of external stakeholders to help shape and inform opinion, conduct research or seek to agree standards with other industry players, as well as provide feedback to shape Vodafone's internal policy." (Deadman and Chandler, 2012) **External - Public Consultation and Involving with Data Subjects** "As a thorough basis for assessing data protection risks, it is of utmost importance to involve not only the controller, IT security experts, and data protection experts, but also individuals with in-depth knowledge of domain-specific workflows and processing activities and their technical		(2012) Waters (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012) Zamorano et al. (2023)

Name	Examples	Files	References
	implementation. It is advisable to involve additional stakeholders or their representatives. This heterogeneity of the working group must be taken into account by a transparent methodological approach." (Friedewald et al, 2022) **External - External PIA Reviews** "Recognising the expertise of the regulator and the usefulness of review and feedback, assessors often deliver the reports in draft form and seek comment. This point in the process is full of promise and opportunity for assessor, organisation, regulator and other stakeholders but also contains risks for several of these. Making the most of this moment is essential for the success of PIA as a modern means for understanding privacy risk and opportunity and managing processes to deliver good privacy outcomes for individuals whether as citizens, consumers, employees or otherwise." (Stewart, 2012)		
05 - Methodological Strengths	**PIAs as a privacy-by-design approach** "Privacy impact assessment may represent a general solution to build robust privacy protective information systems by design." (Di Iorio et al, 2009) **Continuous improvement and streamlining of PIA frameworks, methodologies and tools** "On the other hand, new software tools are released to make the data protection impact assessment more practical and to foster collaboration between stakeholders, and in this study we have applied a free	26	Alaqra et al. (2021) Alaqra et al. (2023) Bayley and Bennet (2012) Brautigam (2012) Deadman and Chandler (2012) Di Iorio et al. (2009) Edwards (2012) Friedewald et al. (2022) Henriksen-Bulmer et al. (2020) Kroener et al. (2021)

Name	Examples	Files	References
	software developed by CNIL." (Rajamäki et al, 2021) **PIAs as a systematic and sound methodology for analysis** "With the data protection impact assessment of the CWA summarized here, a methodological sound form for analyzing, determining, and, if necessary, mitigating the data protection risks of a tracing apps has been presented." (Rehak and Kuhne, 2022) **PIAs considered a widespread practice** "Privacy impact assessments are now commonplace, being commissioned and prepared in respect of a wide range of innovations and proposals." (Edwards, 2012)		McKee (2022) Nas (2019) Rajamäki (2021) Rehak and Kuhne (2022) Schneider et al. (2023) Sharma and Kaushik (2017) Shin et al. (2017) Stewart (2012) Stoddart (2012) Thoma (2012) Vandercruysse et al. (2021) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012)
06 - Increased Transparency to Stakeholders	**PIAs for increased transparency** "The conduct of PIAs, in accordance with existing public policy imperatives, has the benefits of forcing a degree of transparency, enabling informed decision-making and the filtering out of unjustified measures, and leading to the imposition of appropriate controls and mitigation measures on those proposals that are found to be justified." (Clarke, 2016) **Publishing the public PIA reports** "One way to take up and deal with concerns like that is through public debate based on a high quality data	23	Alaqra et al. (2021) Alaqra et al. (2023) Bas Seyyar and Geradts (2020) Bayley and Bennet (2012) Clarke (2016) Dashti et al. (2021) Easton (2017) Edwards (2012) Friedewald et al. (2022) Horák et al. (2019) Nas (2019) Rehak and Kuhne (2022)

Name	Examples	Files	References
	protection impact assessment. By making the official CWA DPIA publicly available, which is not requested by the GDPR, the societal significance of the CWA system was acknowledged and discussing it became possible." (Rehak et al, 2022) **Leverage central PIA registries** "The Canadian Office of the Privacy Commissioner's audit report recommended creation of a central registry of PIAs. It would help people to find a particular PIA which might otherwise be buried on a website." (Wright and De Hert, 2012) **PIAs as a basis for societal discussion of privacy risks** "Furthermore, the DPIA report has received a lot of attention in the media[3] and in the political debate, too. A Dutch member of parliament asked the Dutch Minister of Interior and Kingdom Relations whether the transfer of data to the US could be qualified as a data breach, and whether strategic infor mation could have been leaked to the US." (Nas, 2019)		Rehak et al. (2022) Stewart (2012) Stoddart (2012) Thoma (2012) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012)
07 - Privacy Awareness and Training	**PIA self-assessment for increased privacy awareness in the organisation** "The findings from this study showed that including contextual questions in a practical guided manner within the privacy risk assessment, helped raise awareness of not only what is meant by context in terms of privacy risk assessment, but also identified contextual nuances that might not otherwise be apparent when conducting	18	Bayley and Bennet (2012) Brautigam (2012) Deadman and Chandler (2012) Easton (2017) Henriksen-Bulmer et al. (2020) Horák et al. (2019)

Name	Examples	Files	References
	traditional privacy impact assessments (PIAs)." (Henriksen-Bulmer et al, 2020) **PIAs and the organisational privacy culture** "Based on our study, we found that while PIA was done at the initial stages, this was not enough to assure privacy. The organization adopted a proactive approach to ensure privacy assurance utilizing means such as annual refresh of PIA, trigger-based updates and investing in promoting a privacy culture. Following the conformist strategy alone was not enough for the organization to provide privacy assurance, and it moved to entrepreneur strategy." (Sharma and Kaushik, 2017) **Ensure that staff has PIA and privacy training** "When a great number of initiatives require a PIA, this necessarily leads to those PIAs being completed by people with little knowledge of privacy, or stretching the resources of qualified staff. […] One way to address this is by providing specialised PIA training such as that offered by the government of Canada.[69] Another is to ensure that all staff have some basic privacy training." (Bayley and Bennet, 2012)		Parks et al. (2011) Rehak and Kuhne (2022) Schneider et al. (2023) Sharma and Kaushik (2017) Stoddart (2012) Thoma (2012) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Wright et al. (2014) Wrigth and De Hert (2012)
08 - Risk Management	**PIAs as part of the risk management process** "Third, the adoption of a privacy impact assessment (PIA) allows the integration of a risk management approach to effectively assess the different types of privacy risks. The findings provide evidence for: (1) a gap between privacy responses and their outcomes on healthcare practice and delivery; (2) the importance of the privacy impact assessment as a risk management tool; and (3) the	15	Bayley and Bennet (2012) Deadman and Chandler (2012) Friedewald et al. (2022) Iwaya et al. (2019) Parks et al. (2011) Sharma and Kaushik (2017)

Name	Examples	Files	References
	challenging context of the healthcare environment of how privacy responses are unfolding." (Parks et al, 2011) **PIAs help to identify the people responsible for treating issues and risks in the organisation (privacy risk owners)** "It is an important tool for providing data about issues and risks that need to be treated, and provides a methodology for agreeing and prioritising treatment actions. It is also useful in identifying the correct people within the business who are responsible for treating those issues and risks, as they are likely to be the privacy risk owners rather than the privacy officer or manager." (Deadman and Chandler, 2012)		Stoddart (2012) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012) Zamorano et al. (2023)
09 - Industry Collaboration and Standardisation	**Sharing PIA experience and tools with others outside the organisation** "In addition, it has been mentioned that sharing DPIA practices could increase practitioners' current knowledge, as well as their confidence, while it could also increase DPIAs' actual effectiveness." (Ferra e al, 2020) **Industry professionals see benefits and plan to use PIAs** "One method used to test the models was through industry training sessions where attendees were polled during the training to ask if they currently conduct privacy assessments and if the new methodology was something they would implement and use at their organization. […] Further, 95% responded they would benefit from the new privacy assessment methodology and plan to introduce it	13	Bayley and Bennet (2012) Deadman and Chandler (2012) Ferra et al. (2020) Horák et al. (2019) McKee (2022) Parks et al. (2011) Sharma and Kaushik (2017) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Warren and Charlesworth (2012) Wright et al. (2014) Wrigth and De Hert (2012)

Name	Examples	Files	References
	in their organizations." (McKee, 2022)		
10 - PIAs for Trust and Reputation	**PIAs for building trust and reputation** "The privacy impact assessment, therefore, provides an essential foundation for addressing the three drivers of Vodafone's approach to privacy[25] – trust, reputation and regulation." (Deadman and Chandler, 2012) "Evidently, a strong reputation for data protection can induce citizen trust, but building a reputation is a broader concept.[116] For example: an established data controller publishing a full DPIA report on its website could garner trust from citizens who perceive this as very transparent, while business associates might positively or negatively judge the procedures on a more technical level." (Vandercruysse et al, 2021)	13	Alaqra et al. (2021) Alaqra et al. (2023) Deadman and Chandler (2012) Edwards (2012) Iwaya et al. (2023) Parks et al. (2011) Thoma (2012) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Wadhwa (2012) Wright and Wadhwa (2013) Wright et al. (2014) Wrigth and De Hert (2012)
11 - Accountability	**Develop mechanisms for accountability, monitoring, and internal or external oversight** "Scholars and policy-makers have identified several elements critical to this transformation. First, they cite the development of mechanisms for accountability to external oversight." (Bamberger and Mulligan, 2012) "In some organisations, the [PIA] report was signed off by key parties (like applicable line manager, data protection officer, information security officer and depending on the residual risks also executive management). This not only improved the involvement of the key parties but also the quality of the report." (Van Puijenbroek and Hoepman, 2017)	9	Bamberger and Mulligan (2012) Deadman and Chandler (2012) Edwards (2012) Sharma and Kaushik (2017) Stoddart (2012) Van Puijenbroek and Hoepman (2017) Vandercruysse et al. (2021) Warren and Charlesworth (2012)

Name	Examples	Files	References
			Wrigth and De Hert (2012)
12 - Regulators' Views and Support	**Clearer guidelines for PIAs from data protection authorities are helpful** “As there was a general fear of compliance violations and the corresponding fines, organisations tried to include a broad range of processing activities as requiring a DPIA to be on “the safe side”. In such a situation, it was helpful in providing guidance, especially to those organizations that had hitherto given little attention to data protection issues, that the data protection authorities have compiled authoritative lists of processing operations which are always subject to the requirement to undertake a DPIA (aka “blacklists”).” (Friedewald et al, 2022) **Regulators play a strong advocacy role** “The French DPA said that ‘trust will only be enabled if citizens and/or consumers are confident that PIAs are done seriously, reviewed independently, and that additional data protection safeguards (eg data breach notification, etc.) are implemented. In this regard, data protection authorities have an important role to play’.” (Wright and Wadhwa, 2013)	8	Friedewald et al. (2022) Shin et al. (2017) Stewart (2012) Stoddart (2012) Warren and Charlesworth (2012) Waters (2012) Wright and Wadhwa (2013) Wrigth and De Hert (2012)
13 - PIAs as Competitive Advantage and Cost Reduction	**The benefits of PIAs outweigh the costs** “Use of resources for privacy and security is an issue in all companies, but all experts asked have stated that the benefits of PIAs far outweigh the costs.” (Brautigam, 2012) “By far, most DPAs (Bulgaria, Finland, France, Berlin, Hungary, Ireland, Lithuania, Luxembourg, Netherlands, Poland, Slovenia, Spain, Sweden, the UK) thought that the	8	Bayley and Bennet (2012) Brautigam (2012) Iwaya et al. (2019) Parks et al. (2011) Thoma (2012) Vandercruysse et al. (2021) Wright and Wadhwa (2013)

Name	Examples	Files	References
	advantages of conducting an assessment outweighed the costs of its undertaking." (Wright and Wadhwa, 2013) **PIAs and privacy are seen as a competitive advantage** "Where PIAs are conducted in the private sector, the methods and considerations can be different. Some organisations recognise that privacy can give them a strategic advantage." (Bayley and Bennet, 2012) "Protecting patients' information from external and internal unauthorized access and other threats is considered a competitive advantage." (Parks et al, 2011) "Additionally, the DPIA can be used as a signal from the SCSP demonstrating that their product is safe and that data risks are well-considered." (Vandercruysse et al, 2021)		Wrigth and De Hert (2012)

References

Ahmadian, A.S., Strüber, D., Riediger, V., Jürjens, J., 2018. Supporting privacy impact assessment by model-based privacy analysis, in: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. Presented at the SAC 2018: Symposium on Applied Computing, ACM, Pau France, pp. 1467–1474. https://doi.org/10.1145/3167132.3167288

Alaqra, A.S., Fischer-Hübner, S., Karegar, F., 2023. Transparency of Privacy Risks Using PIA Visualizations, in: Moallem, A. (Ed.), HCI for Cybersecurity, Privacy and Trust, Lecture Notes in Computer Science. Springer Nature Switzerland, Cham, pp. 3–17. https://doi.org/10.1007/978-3-031-35822-7_1

Alaqra, A.S., Kane, B., Fischer-Hübner, S., 2021. Machine Learning–Based Analysis of Encrypted Medical Data in the Cloud: Qualitative Study of Expert Stakeholders' Perspectives. JMIR Hum Factors 8, e21810. https://doi.org/10.2196/21810

Bamberger, K.A., Mulligan, D.K., 2012. PIA Requirements and Privacy Decision-Making in US Government Agencies, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 225–250. https://doi.org/10.1007/978-94-007-2543-0_10
Bas Seyyar, M., Geradts, Z.J.M.H., 2020. Privacy impact assessment in large-scale digital forensic investigations. Forensic Science International: Digital Investigation 33, 200906. https://doi.org/10.1016/j.fsidi.2020.200906
Bayley, R.M., Bennett, C.J., 2012. Privacy Impact Assessments in Canada, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 161–185. https://doi.org/10.1007/978-94-007-2543-0_7
Bräutigam, T., 2012. PIA: Cornerstone of Privacy Compliance in Nokia, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 253–274. https://doi.org/10.1007/978-94-007-2543-0_11
Campanile, L., Forgione, F., Mastroianni, M., Palmiero, G., Sanghez, C., 2022. Evaluating the Impact of Data Anonymization in a Machine Learning Application, in: Gervasi, O., Murgante, B., Misra, S., Rocha, A.M.A.C., Garau, C. (Eds.), Computational Science and Its Applications – ICCSA 2022 Workshops, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 389–400. https://doi.org/10.1007/978-3-031-10542-5_27
Clarke, R., 2016. Privacy impact assessments as a control mechanism for Australian counter-terrorism initiatives. Computer Law & Security Review 32, 403–418. https://doi.org/10.1016/j.clsr.2016.01.009
Dashti, S., Santana de Oliveria, A., Kaplan, C., Dalcastagnè, M., Ranise, S., 2021. Can Data Subject Perception of Privacy Risks Be Useful in a Data Protection Impact Assessment?:, in: Proceedings of the 18th International Conference on Security and Cryptography. Presented at the 18th International Conference on Security and Cryptography, SCITEPRESS - Science and Technology Publications, Online Streaming, --- Select a Country ---, pp. 827–832. https://doi.org/10.5220/0010602608270832
Deadman, S., Chandler, A., 2012. Vodafone's Approach to Privacy Impact Assessments, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 285–304. https://doi.org/10.1007/978-94-007-2543-0_13
Di Iorio, C.T., Carinci, F., Azzopardi, J., Baglioni, V., Beck, P., Cunningham, S., Evripidou, A., Leese, G., Loevaas, K.F., Olympios, G., Federici, M.O., Pruna, S., Palladino, P., Skeie, S., Taverner, P., Traynor, V., Benedetti, M.M., 2009. Privacy impact assessment in the design of transnational public health information systems: the BIRO project. Journal of Medical Ethics 35, 753–761. https://doi.org/10.1136/jme.2009.029918

Easton, C., 2017. Analysing the Role of Privacy Impact Assessments in Technological Development for Crisis Management. J Contingencies Crisis Man 25, 7–14. https://doi.org/10.1111/1468-5973.12140
Edwards, J., 2012. Privacy Impact Assessment in New Zealand – A Practitioner's Perspective, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 187–204. https://doi.org/10.1007/978-94-007-2543-0_8
Ferra, F., Wagner, I., Boiten, E., Hadlington, L., Psychoula, I., Snape, R., 2020. Challenges in assessing privacy impact: Tales from the front lines. Security and Privacy 3. https://doi.org/10.1002/spy2.101
Friedewald, M., Schiering, I., Martin, N., Hallinan, D., 2022. Data Protection Impact Assessments in Practice: Experiences from Case Studies, in: Katsikas, S., Lambrinoudakis, C., Cuppens, N., Mylopoulos, J., Kalloniatis, C., Meng, W., Furnell, S., Pallas, F., Pohle, J., Sasse, M.A., Abie, H., Ranise, S., Verderame, L., Cambiaso, E., Maestre Vidal, J., Sotelo Monge, M.A. (Eds.), Computer Security. ESORICS 2021 International Workshops, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 424–443. https://doi.org/10.1007/978-3-030-95484-0_25
Henriksen-Bulmer, J., Faily, S., Jeary, S., 2020. DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems. Future Internet 12, 93. https://doi.org/10.3390/fi12050093
Horák, M., Stupka, V., Husák, M., 2019. GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform, in: Proceedings of the 14th International Conference on Availability, Reliability and Security. Presented at the ARES '19: 14th International Conference on Availability, Reliability and Security, ACM, Canterbury CA United Kingdom, pp. 1–8. https://doi.org/10.1145/3339252.3340516
Iwaya, L.H., Babar, M.A., Rashid, A., Wijayarathna, C., 2023. On the privacy of mental health apps: An empirical investigation and its implications for app development. Empir Software Eng 28, 2. https://doi.org/10.1007/s10664-022-10236-0
Iwaya, L.H., Fischer-Hübner, S., Åhlfeldt, R.-M., Martucci, L.A., 2019. Mobile Health Systems for Community-Based Primary Care: Identifying Controls and Mitigating Privacy Threats. JMIR Mhealth Uhealth 7, e11642. https://doi.org/10.2196/11642
Kroener, I., Barnard-Wills, D., Muraszkiewicz, J., 2021. Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems. Ethics Inf Technol 23, 7–18. https://doi.org/10.1007/s10676-019-09501-6
McKee, L., 2022. Privacy Assessment Breakthrough: A Design Science Approach to Creating a Unified Methodology (Doctoral Dissertation). Dakota State University.

Nas, S., 2019. Practitioner's Corner • Data Protection Impact Assessment: Assessing the Risks of Using Microsoft Office ProPlus. European Data Protection Law Review 5, 107–113. https://doi.org/10.21552/edpl/2019/1/17
Parks, R., Chu, C., Xu, H., Adams, L., 2011. Understanding the Drivers and Outcomes of Healthcare Organizational Privacy Responses.
Pribadi, I.L., Suryanegara, M., 2017. Regulatory recommendations for IoT smart-health care services by using privacy impact assessment (PIA), in: 2017 15th International Conference on Quality in Research (QiR) : International Symposium on Electrical and Computer Engineering. Presented at the 2017 15th International Conference on Quality in Research (QiR): International Symposium on Electrical and Computer Engineering, IEEE, Nusa Dua, pp. 491–496. https://doi.org/10.1109/QIR.2017.8168535
Rajamäki, J., 2021. Design Science Research Towards Ethical and Privacy-Friendly Maritime Surveillance ICT Systems, in: Tagarev, T., Atanassov, K.T., Kharchenko, V., Kacprzyk, J. (Eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies, Studies in Big Data. Springer International Publishing, Cham, pp. 95–115. https://doi.org/10.1007/978-3-030-65722-2_7
Rehak, R., Kuhne, C.R., 2022. The Processing goes far beyond "the app" – Privacy issues of decentralized Digital Contact Tracing using the example of the German Corona-Warn-App, in: 2022 6th International Conference on Cryptography, Security and Privacy (CSP). Presented at the 2022 6th International Conference on Cryptography, Security and Privacy (CSP), IEEE, Tianjin, China, pp. 16–20. https://doi.org/10.1109/CSP55486.2022.00011
Rehak, R., Kühne, C.R., Bock, K., 2022. Analysis and Constructive Criticism of the Official Data Protection Impact Assessment of the German Corona-Warn-App, in: Gryszczyńska, A., Polański, P., Gruschka, N., Rannenberg, K., Adamczyk, M. (Eds.), Privacy Technologies and Policy, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 119–134. https://doi.org/10.1007/978-3-031-07315-1_8
Schneider, B., Asprion, P.M., Misyura, I., Jonkers, N., Zaugg, E., n.d. Persona-oriented Data Protection Impact Assessment for Small Businesses. Presented at the Proceedings of Society 5.0 Conference 2023, pp. 152–139. https://doi.org/10.29007/5lfs
Sharma, C., Kaushik, A., 2017. Strategy for privacy assurance in offshoring arrangements. JGOSS 10, 232–254. https://doi.org/10.1108/JGOSS-10-2016-0030
Shin, S., Seto, Y., Sasaki, M., Sakamoto, K., 2017. Analysis of Specific Personal Information Protection Assessment in the Social Security and Tax Number System of Local Governments in Japan, in: Saeed, K., Homenda, W., Chaki, R. (Eds.), Computer Information Systems and Industrial Management, Lecture

Notes in Computer Science. Springer International Publishing, Cham, pp. 685–696. https://doi.org/10.1007/978-3-319-59105-6_59
Stewart, B., 2012. Privacy Impact Assessment: Optimising the Regulator's Role, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 437–444. https://doi.org/10.1007/978-94-007-2543-0_21
Stoddart, J., 2012. Auditing Privacy Impact Assessments: The Canadian Experience, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 419–436. https://doi.org/10.1007/978-94-007-2543-0_20
Thoma, F., 2012. How Siemens Assesses Privacy Impacts, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 275–284. https://doi.org/10.1007/978-94-007-2543-0_12
Todde, M., Beltrame, M., Marceglia, S., Spagno, C., 2020. Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems. Informatics in Medicine Unlocked 19, 100361. https://doi.org/10.1016/j.imu.2020.100361
van Puijenbroek, J., Hoepman, J.-H., 2017. Privacy Impact Assessment in Practice, in: Ceur Workshop Proceedings, (2017)Alamo, J.M. Del (Ed.), IWPE 2017: International Workshop on Privacy Engineering: Proceedings of the 3rd International Workshop on Privacy Engineering, Co-Located with 38th IEEE Symposium on Security and Privacy (S&P 2017). Presented at the IWPE 2017: International Workshop on Privacy Engineering, San Jose (CA), pp. 1–8.
Vandercruysse, L., Buts, C., Dooms, M., 2020. A typology of Smart City services: The case of Data Protection Impact Assessment. Cities 104, 102731. https://doi.org/10.1016/j.cities.2020.102731
Vandercruysse, L., Dooms, M., Buts, C., 2021. The DPIA: Clashing Stakeholder Interests in the Smart City?, in: Data Protection and Privacy: Enforcing Rights in a Changing World. Hart Publishing, p. 245. https://doi.org/10.5040/9781509954544
Wadhwa, K., 2012. Privacy impact assessment reports: a report card. info 14, 35–47. https://doi.org/10.1108/14636691211223210
Warren, A., Charlesworth, A., 2012. Privacy Impact Assessment in the UK, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 205–224. https://doi.org/10.1007/978-94-007-2543-0_9
Waters, N., 2012. Privacy Impact Assessment – Great Potential Not Often Realised, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 149–160. https://doi.org/10.1007/978-94-007-2543-0_6

Wright, D., De Hert, P., 2012. Findings and Recommendations, in: Wright, D., De Hert, P. (Eds.), Privacy Impact Assessment. Springer Netherlands, Dordrecht, pp. 445–481. https://doi.org/10.1007/978-94-007-2543-0_22
Wright, D., Wadhwa, K., 2013. Introducing a privacy impact assessment policy in the EU member states. International Data Privacy Law 3, 13–28. https://doi.org/10.1093/idpl/ips029
Wright, D., Wadhwa, K., Lagazio, M., Raab, C., Charikane, E., 2014. Integrating privacy impact assessment in risk management. International Data Privacy Law 4, 155–170. https://doi.org/10.1093/idpl/ipu001
Zamorano, M.M., Newton, N., Bertelli, V., Petersen, L., 2023. Privacy by Design in CBRN Technologies Targeted to Vulnerable Groups: The Case of PROACTIVE, in: Gjøsæter, T., Radianti, J., Murayama, Y. (Eds.), Information Technology in Disaster Risk Reduction, IFIP Advances in Information and Communication Technology. Springer Nature Switzerland, Cham, pp. 244–258. https://doi.org/10.1007/978-3-031-34207-3_16