Privacy and the Holocaust – How Can We Prevent Data Protection from Obstructing Justice and Truth?

Arye Schreiber

Holocaust researchers have long pointed out how European data protection law, ostensibly put in place to protect the rights of individual data subjects, has placed hurdles in the way of their research. A social historian of Nazism, Detlef Mühlberger, after detailing a number of archives that placed varying restrictions on what he could access and copy, succinctly summarized how evolving data protection law might stifle this form of historical research:

> I fear that in [the] future, changes in the application of laws relating to data protection made urgent by the appearance of computerized data banks may be used by some of the political masters of *Länder* archives to prevent access to personal files on members of the NSDAP, the SA, the SS, and so on, a possible development which the academic community must challenge and resist collectively.[1]

These words were written almost three decades ago and they were prescient. In a previous article,[2] the present author has expanded on the problem expressed by Mühlberger, namely that data protection may obstruct history, truth and justice. As such, European data protection law has been a major obstacle to Holocaust research. The principle of data privacy was claimed and abused to block bank and insurance restitution, to obstruct archives from being opened, and to prevent opportunities to pursue justice directly against perpetrators.

The present article aims to contribute to a possible solution, and considers ways in which Holocaust research institutions may react to overcome the challenges of data protection law. The appendix to this article presents a proposed joint position for Holocaust research institutions to broach European data protection law as it affects Holocaust research and archiving.

Background

In December 2015, the High Court of Rostock, in the north German state of Mecklenburg-Vorpommern, found that Hubert Zafke, now aged 98, was fit to stand trial as an accessory to 3,681 murders committed during his time as a paramedic in Auschwitz in 1943-44. By August 2017, the prosecutors conceded that Zafke was no longer fit to stand trial and the case was closed. Given the age of any possible surviving perpetrators, the end of the Zafke trial may mark the end of all trials of Holocaust perpetrators.

The sensations of Holocaust trials are now essentially over, but the challenges of Holocaust research, evidence, and education are not. Holocaust research institutions are deeply involved in education and training, historical research, and digitization for posterity. New avenues to Holocaust research largely capitalize on the power of various data tools—artificial intelligence for translation and identification, big data research on Holocaust movement and more, and these appear to bring much of the underlying material within the scope of data protection law.

On May 25, 2018, the EU's General Data Protection Regulation (GDPR) entered into force.[3] This law creates

1. Detlef Mühlberger, Hitler's Followers: Studies in the Sociology of the Nazi Movement (1991), p. 4.
2. Arye Schreiber, The Duty to Remember v. the Right to be Forgotten: Holocaust Archiving and Research, and European Data Protection Law, IX Holocaust — Studii și Cercetări (2017), pp. 140-190.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

new challenges for Holocaust archiving and research.[4] For example, after GDPR's initial draft was published, it became apparent that this law could be used to dramatically restrict researchers' access to Holocaust archives. The International Holocaust Remembrance Alliance (IHRA) looked into the possible ramifications of GDPR for Holocaust research and reached some disturbing conclusions: "After two years of research and analysis, IHRA had determined definitively that researchers and research organizations were already being denied access to Holocaust-related materials on the premise that the GDPR would not permit the use of these materials, despite the fact that the regulation had not yet been adopted."[5] Acting on this finding, IHRA led an effort to influence the drafting of GDPR, culminating in an important addition to GDPR—Recital 158 of its final version, which empowers EU member states to legislate specific terms for Holocaust material. In this article, we will consider ways in which, working within the confines of GDPR's substantive provisions, Holocaust archiving may be facilitated rather than obstructed.

The three key topics for analysis in this article are: (i) is Holocaust archive material "personal data" within the meaning in GDPR? I will suggest that entire collections may not be; (ii) are Holocaust victims and survivors "data subjects" within the meaning in GDPR? I will propose a reasonable assumption that they are not, unless proven to be alive; and (iii), does GDPR provide mechanisms that enable data processing, including publication, without the consent of the data subjects? I will suggest that it provides several. Before addressing these topics, we may first look to an alternate model, one of general suspension of privacy rights following mass disasters.

Can Privacy Be Suspended in the Search for Justice?

Major international human rights instruments such as the Universal Declaration of Human Rights (Article 12), and the European Convention on Human Rights (Article 8) protect privacy. Yet where there are conflicting values, privacy is frequently and rightly trumped, and the GDPR itself (Recital 4) stipulates that the processing of personal data must be balanced against other fundamental rights:

> The processing of personal data should be designed to serve humanity. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights…

Privacy was not suspended in the search for Holocaust justice and truth, but on the contrary, was typically reinforced and abused as an obstacle to Holocaust truth, justice and restitution. GDPR does not have a mechanism for suspending privacy rights—as some other laws do, as discussed below, but rather purports to balance data protection with other rights in its provisions. The experience of the last 30 years ought to lead to an alternate conclusion and approach, enabling a general suspension of privacy in the wake of disaster and mass atrocity. There are national and international processes, movements and events that loom so large as to trump privacy rights. This was a conclusion reached in several former communist regimes in their search for truth and justice after the fall of communism. For example, Slovakia's Nation's Memory Institute (NMI), founded after the fall of communism in Slovakia, took a bold position of publishing comprehensive lists of both victims and perpetrators of secret police action throughout the communist era. This resulted in many court proceedings, brought particularly by alleged perpetrators exposed by the NMI who claimed that they were unfairly or falsely included in the lists of collaborators. In some cases, for example, it was shown that people who had in fact not collaborated with the secret police were recorded as collaborators without their knowledge or consent, principally because they had inadvertently provided some useful information, or were thought to be able to do so. By all appearances, some personal wrongs had to be righted in the aftermath of publication, but the revelations were central to the lustration, to the truth and reconciliation, in post-communist Slovakia. Likewise, in 2006 the NMI "published a register of Jewish population from 1942, which it considers to be 'the most important document containing

4. Various legislative provisions and precedent in other jurisdictions create similar, or further, challenges for Holocaust research, though discussion of other legal instruments is beyond the scope of this article.
5. Reference to the Holocaust in GDPR, International Holocaust Remembrance Alliance, Dec. 18, 2015, available *at* https://www.holocaustremembrance.com/stories/reference-holocaust-gdpr (last visited July 5, 2018).

information about the Holocaust victims in Slovakia'."[6] According to Kovanic, the "right of protection of personality can be legally suspended in the case that the law aims at some other, higher purpose…. The right to know the truth is such a purpose in the case of Slovakia."[7] This is bold and refreshing, and in my view, a model to be emulated. Similar models were developed in other countries, and in others still, this position was argued for, but not ultimately adopted.

In Hungary, privacy was a clear constraint on publication of lustration data.[8] In Poland, the matter was considered by a Constitutional Tribunal, which ruled that political party affiliations and past convictions were to be protected as sensitive data. The court ultimately found that prior to publication, each file in the archives in question would need to be reviewed and sensitive data redacted, a project for which resources were ostensibly not available, and as a result, "the issue of privacy and protecting sensitive data becomes a central problem in the opening of the archives to the public."[9] Former Polish Commissioner for Data Protection, Ewa Kulsza, wrote of former collaborators teaching in university: "Those who refused [to divulge information on whether or not they were collaborators] because of protecting their own privacy faced being unemployed. Those who confessed of [sic] being collaborators, could stay."[10] This anecdote reflects the ironic situation in which collaborators could be forgiven for collaboration, but not for secrecy. Where a major process of truth, healing and justice is underway, the lack of transparency is harmful to the process as a whole, whereas the particular collaboration of one person or another may be of minimal consequence. This expectation of transparency was, of course, completely lacking in all jurisdictions post-Holocaust. Several East European countries specifically learned from the Holocaust experiences when determining the rules, including the data protection rules that would govern their lustration processes. The Slovakian law establishing the NMI opened with Santayana's "He who ignores history is doomed to repeat it," and specifically drew on the Holocaust precedent and experience before giving the NMI the power to access any document, data protection notwithstanding.[11]

The debate regarding revelations of Holocaust era atrocities has parallels in lustration processes in post-communist Eastern Europe and elsewhere. A sweeping waiver of privacy rights in relation to the Holocaust may have been relevant in the immediate aftermath of the Holocaust; but with the passage of time, it has lost its urgency. Today, laws of this kind enable suspension of privacy, temporarily in disaster zones.

In 2017, Hurricane Harvey left large parts of Houston, Texas underwater, causing 88 deaths and U.S. $125B in damage. The United States Department of Health and Human Services issued a notice that, as a result of this disastrous situation, several core rights and duties under the Health Insurance Portability and Accountability Act 1996 (HIPAA) were waived, including "the requirements to obtain a patient's agreement to speak with family members or friends involved in the patient's care."[12] This waiver had clear limits—applying only in the disaster zone, to hospitals following emergency protocols, and only for a limited time. Under GDPR, there is no body that has the power to issue such a statement, but the vital interests of a data subject or a third person form a lawful basis for data processing.[13]

---

6. Martin Kovanic, Files and Privacy: Challenges of Transitional Justice in Slovakia, Studia Universitatis Cibiniensis, Series Historica, vol. XI (2014), pp.113-132.
7. *Ibid*, p.124.
8. Vladimíra Dvořáková, Lustration and Consolidation of Democracy and the Rule of Law in Central and Eastern Europe (2007), p. 38.
9. Magdalena Kaj, Megan Metzger, Justice or Revenge? The Human Rights Implications of Lustration in Poland, available *at* https://www.humanityinaction.org/knowledgebase/165-justice-or-revenge-the-human-rights-implications-of-lustration-in-poland (last visited July 5, 2018). The ECtHR eventually found that the Polish lustration process violated ECHR Article 6 rights. Matyjek v. Poland, ECtHRApp. no. 38184/03, (2007). *See* discussion in Samuel Issacharoff, Managing Conflict through Democracy, Rights in Divided Societies (Colin Harvey, Alex Schwartz, eds., 2012), p. 48.
10. Ola Svenomius, Fredrika Bjorklund, and Pawel Waszkiewicz, Surveillance, Lustration and the Open Society: Poland and Eastern Europe, Histories of State Surveillance in Europe and Beyond (Kees Boersma, Rosamunde van Brakel, Chiara Fonio, Pieter Wagenaar, eds., 2014), p.106.
11. *See* full discussion in Vladimíra Dvořáková, The Institute of National Memory: Historical Memory as a Political Project, Lustration and Consolidation of Democracy and the Rule of Law in Central and Eastern Europe (Vladimíra Dvořáková and Andelko Milardović, eds., 2007).
12. Limited Waiver of HIPAA Sanctions and Penalties During a Declared Emergency, US Department of Health and Human Services, available *at* https://www.hhs.gov/sites/default/files/hurricane-harvey-hipaa-bulletin.pdf (last visited July 5, 2018).
13. EU GDPR Articles 6.1(d), 9(2)(c).

More generally, the 37th International Conference of Data Protection and Privacy Commissioners met in Amsterdam in 2015, and passed resolutions regarding privacy in international humanitarian action.[14] In fulfillment of one of the resolutions of that meeting, privacy experts, including the head of data protection for the International Committee of the Red Cross, prepared a guidebook on data protection for humanitarian agencies. This document clarifies that data protection must not get in the way of humanitarian relief but that on the contrary, they serve the same objective. "Data protection principles should never be interpreted in a way that hampers essential humanitarian work, and should always be interpreted in a way that furthers the ultimate objective of Humanitarian Action, namely safeguarding the life, integrity and dignity of victims of Humanitarian Emergencies."[15] GDPR Article 6(1)(d) states that processing will be lawful if "processing is necessary in order to protect the vital interests of the data subject or of another natural person." Recital 46 gives examples: epidemics, humanitarian disasters, man-made disasters. The Holocaust certainly qualifies as a man-made disaster, but processing of Holocaust-era data is unlikely to be a matter of life and death any more. It therefore remains to be examined if the processing, and especially publication, of Holocaust archives are governed and prevented by GDPR. To examine this question, we will analyze three important points: whether Holocaust archive data relate to identifiable individuals; whether they relate to "data subjects" who are living natural persons; and assuming they relate to identifiable data subjects, whether under GDPR there is a lawful basis in processing them.

Do Holocaust Archives Relate to an Identifiable Natural Person?

GDPR Article 4(1) defines "personal data" as:

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The vast majority of Holocaust victims were murdered without records of their names, or, where records were kept, they were often systematically destroyed. Enormous resources have been – and continue to be – expended in an attempt to identify Holocaust victims. Yet, though some names are known, the name generally does not suffice to identify the person. The *Central Database of Shoa Victims' Names* run by Yad Vashem includes 6.5 million records, but Yad Vashem estimates that there are names of only 4.5 million victims, given the multiple reports of many victims (http://yvng.yadvashem.org/). For example, the present author's great-grandfather seems to have been reported by at least three people. However, there is really no way for Yad Vashem to cross-check all the testimonies and prevent multiple listings, given the vast number of names, the similarities between many of them, the differences in spelling in different languages and even in the same language, and the generally partial or speculative information regarding the death of the victims. Verifying the identity of victims reported several times would require inordinate resources, and in many cases would be impossible. Very often, then, a name is not an identifier, and that has been the position of Yad Vashem in this regard. In some cases, research may uncover the exact identity and fate of a named person, but it is certainly not possible to find everyone, and the expense would be prohibitive. The expense is what makes much of this data non-personally-identifiable. GDPR's Recital 26 specifically explains that the determination of whether data are identifiable will depend on the time and resources required to make the identification:

> To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

14. Resolution on Privacy and International Humanitarian Action, Oct. 27, 2015, available *at* https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf (last visited July 5, 2018).
15. Handbook on Data Protection in Humanitarian Action (Christopher Kuner, Massimo Marelli, eds., 2017), available *at* http://brusselsprivacyhub.eu/publications/dataprotectionhandbook.html (last visited July 5, 2018), p. 15.

Over more than seven decades, very significant resources were dedicated to identifying Holocaust victims, and where data are not known to be tied to a given individual, there is a reasonable assumption to be made that the data are not identifiable, and therefore not "personal data" and not protected by GDPR.

Do the Data Relate to a Living Natural Person?

GDPR is explicit in that it does not govern the data of deceased persons (Recital 27):

> This Regulation does not apply to the personal data of deceased persons.[16] Member States may provide for rules regarding the processing of personal data of deceased persons.

The second sentence specifically empowers EU member states to legislate in this regard, and several have done so. In Hungary, Italy and Spain the families of the deceased are granted limited data subject access rights. In France, data subjects may set down rules that govern their data post mortem. In Denmark and Estonia, the deceased have rights for many years following their death. Setting aside these interesting exceptions, the general rule that applies in the UK, Germany, Poland and elsewhere, is that the deceased have no GDPR rights.

GDPR does not directly discuss the question of how to relate to a person not known to be alive. Given the frightful statistics of Holocaust survival, Holocaust institutions may reasonably claim that the victims are presumed dead unless demonstrated to be alive. One approach is to leave the burden of proving a data subject's existence with the data subject. Anyone claiming data subject rights must demonstrate that there is a data subject (i.e. the claimant) and their identity (Recital 64). Clearly, where someone demonstrates that data relate to them, their rights must be respected, though the rights in the case of historical and scientific research are limited (Article 89). In the case of Holocaust archives, the data subjects were known to have been alive, but persons whose names were taken from Holocaust archives—typically data relating to ghettos and camps— including post-liberation displaced person camps, are very unlikely to be alive. This is true because the survival rates were so poor, and the 73 years that have passed mean that proportionally very few of the then survivors are still alive. Various post-Holocaust compensation programs, notably the International Commission on Holocaust Era Insurance Claims, specifically adopted "relaxed standards of proof"[17] of death of Holocaust victims, and twenty years later, a still more relaxed standard ought to apply.

Another approach is to consider the question of data subjects who may or may not be alive, as a general part of the risk assessment required under Recital 76:

> The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

The greater the risks to individuals from the processing in question, the higher the bar will be to prove the data subjects are not alive. For example, if there is a list of victims of sterilization experiments, that may reveal highly sensitive medical information, and ought to be subject to increased safeguards.

In order to give some color to the difficulties and resources required to ascertain a potential data subject's identity and therefore rights, consider the recently discovered diary of one Rywka Lipszyc. Born in 1928, Rywka was held in Lodz, and transported to Auschwitz, where a Red Army doctor found her diary in the rubble of the crematoria. The diary remained in that doctor's possession until she passed away, and her daughter found it and brought it to light.[18] Researchers sought to identify the author, but soon discovered that there were no less

16. Note that Recital 158 states that "this Regulation should not apply to deceased persons." Recital 27 excludes applicability of GDPR to the data of deceased persons; Recital 158 excludes the applicability of GDPR to deceased persons, not to the data.
17. Steven Less, International Administration of Holocaust Compensation: The International Commission on Holocaust Era Insurance Claims (ICHEIC), 9 German Law Journal (2008), pp.1651, 1668.
18. Dan Pine, The diary of another young girl: Holocaust journal comes to light in San Francisco, Jewish News of Northern California, March 14, 2014, available *at* https://www.jweekly.com/2014/03/14/the-diary-of-another-young-girl-holocaust-journal-comes-to-light-in-san-fra/ (last visited July 5, 2018).

than 22 recorded Lodz prisoners with that name.[19] They appealed for more information in the hope of identifying the right person, and eventually identified the author as one Rywka Bajla Lipszyc, based on details in the diary. Rywka Bajla Lipszyc survived Auschwitz, was transferred to Gross-Rosen, and survived the death march to Bergen Belsen, and the last record of her was hospitalization shortly after liberation, September 10, 1945. Since then, all trace of her was lost. We do not know if she is alive, or even whether she survived for any time after her hospitalization. If she had survived, she would be 90 today. Is such a diary to be treated as personal data? It took years to identify the author, even once her first and last name were known. Now that we know the author, can we assume that she is not alive? She was a survivor, by any measure, but even if we assume she survived beyond that hospitalization, it is very unlikely that she is still alive today.

In summary, institutions may be able to take the position that all data subjects are deceased unless known otherwise, or that it can be determined otherwise at reasonable cost. Except where particularly sensitive data are known about a particular individual, it may be assumed the Holocaust data subject is not alive and therefore, in most jurisdictions, their data are not protected by GDPR.

Is There a Lawful Basis for Processing Holocaust Archives?

Assuming that in particular circumstances GDPR does in fact apply, would processing of personal data of Holocaust victims and perpetrators be lawful? GDPR Article 6 provides a closed list of alternate bases for the lawfulness of processing of personal data. Several of these bases are of particular interest, each considered in turn: Article 6(1)(c), (e) and (f) are each discussed, though not in that order.

GDPR Article 6(1)(f) provides a mechanism of "legitimate interest," which is of particular relevance for Holocaust institutions. Article 6(1)(f) states that processing is lawful if it is

> necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The rule is that the processing must be for the purposes of legitimate interests, with a caveat that it will not apply where such interests are overridden by the interests or fundamental rights of the data subject. As to the rule, the CJEU recently clarified the meaning of "legitimate interests" in *Rīgas* (C-13/16). The details of the case are not relevant here. Broadly, the court broke down the "legitimate interests" basis, under the then current data protection directive, into three questions (the first rather circular): is the interest a legitimate one; is processing necessary to pursue that interest; and do others' rights and freedoms trump those legitimate interests. Holocaust research and education, memorialization, family reunion, property restitution and other ends to which Holocaust research is carried out are clearly a legitimate interest for institutions.[20] The processing of Holocaust archives is certainly necessary for the pursuit of that legitimate interest. It is the third question that is hardest: are data subjects' rights and freedoms adversely affected?[21] GDPR clarifies (Recital 47) that this question is to be assessed "taking into consideration the reasonable expectations of data subjects based on their relationship with the controller." For some survivors, revelation as a Holocaust victim and survivor may in itself pose certain threats to rights and freedoms. It may expose survivors to deniers and neo-Nazis; it may reveal personal information—say health information, sexual orientation or other sensitive data. However, overwhelmingly it seems that the reverse is true. Methodical research of this point is required, but based on cursory investigation with multiple institutions engaged in Holocaust research, there could barely be found a handful of instances in which a Holocaust survivor had objected to online publication of their Holocaust details

19. Litzmannstadt Ghetto mystery to be solved: Can you help? (The Marek Edelman Dialogue Center in Lodz), available *at* https://www.centrumdialogu.com/en/litzmannstadt-ghetto/77-ghetto-litzmannstadt/archiwum-aktualnoci/646-ktokolwiek-widzial (last visited July 5, 2018).
20. EU Commission's Working Party 29 (since renamed European Data Protection Board) in its Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, published April 9, 2014, provided a non-exhaustive list of legitimate interests, and included "processing for historical, scientific or statistical purposes" (para. III.3.1, p. 25).
21. Consideration of the rights and freedoms of Holocaust perpetrators is not considered here, for several reasons; for the present purpose, it suffices to note that there is plainly a public interest that justifies that processing; *see* EU GDPR Recital 50.

and experiences. These few cases each had an additional dimension, and never involved survivors who specifically had not wanted their story published. For example, one Jewish survivor had hidden his Jewish identity and lived as a Gentile since liberation. Another agreed to have her testimony available to the public, but did not want it published online. In any case, the rate of objections to any form of publication, for any reason at all, appears to be somewhere between 1/10,000 and 1/100,000, and as such, not deserving of protection, except where a specific data subject has made claims in that regard. The present authors has likewise interviewed a number of survivors of various Holocaust horrors, and in every instance, the interviewees said that they have a strong interest in publication, rather than restriction of publication.

The desire of survivors to have their story told, their experiences published, has been a driving force in several massive initiatives in historical evidence collection and publication, such as the USC Shoah Foundation Institute for Visual History and Education, and others. The need to preserve and publish Holocaust experiences sometimes overwhelms very specific duties of privacy. Most famously, consider Anne Frank's diary.

> SATURDAY, JUNE 20, 1942: Writing in a diary is a really strange experience for someone like me. Not only because I've never written anything before, but also because it seems to me that later on neither I nor anyone else will be interested in the musings of a thirteen- year- old schoolgirl. Oh well, it doesn't matter. I feel like writing, and I have an even greater need to get all kinds of things off my chest.
> "Paper has more patience than people." I thought of this saying on one of those days when I was feeling a little depressed and was sitting at home with my chin in my hands, bored and listless, wondering whether to stay in or go out. I finally stayed where I was, brooding. Yes, paper does have more patience, and since I'm not planning to let anyone else read this stiff-backed notebook grandly referred to as a "diary," unless I should ever find a real friend, it probably won't make a bit of difference.

Anne wrote her diary for herself, and expressly wrote that she was "not planning to let anyone else read this …diary." Nonetheless, her own father, who had personally promised her that he would never read her diary,[22] understood that publishing Anne's diary was a way not only of fulfilling her desire to become a writer, but more importantly to memorialize her and her experiences.[23]

Other older diarists specifically wrote in the hope that they would be remembered by their words and memorialized by them.[24] Miriam Chaszczewacki, for example, lived and kept a diary in the Rodomsko Ghetto. She was murdered in Treblinka in 1942 at the age of eighteen. Her diary expressly testifies to her desire to have it made public:

> It may seem silly, but only a step away from death I still worry about my diary. I would not want for it to meet a miserable end in an oven or on a rubbish heap. I wish somebody could find it—even if it be only a German—and would read it. I wish that these scribblings, though they record barely a fraction of the cruelties, would one day serve as a true and faithful document of our times.[25]

Diarists may be a group with a predilection to writing for publication and posterity, though in Anne Frank's diary that may not have been the case. Others kept notes and even built archives with the specific aim of saving

---

22. *See* his televised interview, available *at* https://www.youtube.com/watch?v=AWRBinP7ans (last visited July 5, 2018).
23. Otto Frank held back a number of pages from publication because he thought they violated others' privacy, in particular pages relating to Anne's emerging sexuality; to her parents' strained marriage; to Miep's fiancé; and finally to the fact that she clearly did not want her diary published. Curiously, these various pages led to their own legal wrangling: Ralph Blumenthal, Five Precious Pages Renew Wrangling over Anne Frank, NY Times, Sept. 10, 1998, available *at* https://www.nytimes.com/1998/09/10/world five-precious-pages-renew-wrangling-over-anne-frank.html (last visited July 5, 2018).
24. For discussion and some examples, *see* Amos Goldberg, Trauma in the First Person: Diary Writing During the Holocaust (2017), e.g., p. 147 regarding Klemperer's diary written with the express purpose of bearing witness.
25. Stefania Heilbrunn, Children of Dust and Heaven: A Diary from Nazi Occupation Through the Holocaust (2013), p. 133.

the evidence for posterity. Marcel Nadjari was able to write notes during the horrors of the *sonderkommando* at Auschwitz. He buried the papers and survived Auschwitz and later Mathausen, and died in 1971. His papers were unearthed years later.[26] More famously, the "Oneg Shabbat" archive of the Warsaw Ghetto was built by a team led by Emanuel Ringelblum, the Jewish historian of Polish Jewry. It was compiled precisely with a view to telling the story which the Nazis would later deny and to which there would be few witnesses.

In the confines of this article, just a small sample of anecdotal evidence has been presented for the need for publication, and the manner in which it rightly overwhelms privacy. The dignity of the data subject is much better served in these cases by publication than by data protection. In such situations, we must be wary of those who claim to defend the privacy rights of victims, especially of victims who have not made that claim themselves. This is what Anita Allen calls Paternalistic Privacy, where privacy is imposed, rather than demanded:

> Government can turn privacy into a weapon against its own citizens and charges. Government can coerce privacy to reduce the transparency of its operations and accountability of its officials. A problem arises when government seeks to avoid transparency by imposing privacy, using individual privacy rights as a pretextual grounds for withholding information the public or its representatives have a right to know.[27]

The same may apply to institutions, and even to individuals, claiming privacy for those who do not claim it for themselves. There is unquestionably a "legitimate interest" in publishing Holocaust archives, with the caveats set in the law, notably that such processing may not override the rights and freedoms of the data subjects, and no institution—legal, law enforcement, regulatory, or social—ought to be allowed to claim otherwise on behalf of survivors.

Above I argued that there is a legitimate interest in processing personal data in the context of Holocaust research, and that—assuming the data relate to living data subjects—it would thus be justified under the legitimate interest doctrine.

A second lawful basis that may apply in these circumstances is public interest. GDPR Article 6(1)(e) provides that processing is lawful if it "is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller." Article 6(3) further provides that this basis may be laid down only by either EU law, or by the member state law to which the Controller is subject. Some member states do have laws governing Holocaust research and archive institutions. For example, the Polin Museum, Poland's Museum of the History of Polish Jews—which though not a Holocaust museum as such, does include Holocaust research—was formed and funded, and is governed, by member state legislation.[28]

An additional lawful basis may be GDPR Article 6(1)(c), which states that processing is lawful if it "is necessary for compliance with a legal obligation to which the controller is subject." Note that, in contrast with Article 6(1)(e) discussed in the previous paragraph, this basis is not qualified by the need for the member state or union law. Rather it may apply to non-member-state law, such as the laws that established Yad Vashem or USHMM.[29]

Summary and Next Steps

It has been argued here that many Holocaust era archives and collections will not include protected "personal data" under GDPR. The data may be personal in an ordinary sense, but not in the legal sense, since they cannot identify an individual. Moreover, even where the data could identify an individual, that person may be presumed to be no longer alive, unless it is shown otherwise. Finally, even where the data are in fact governed by GDPR, there

---

26. Laurence Peter, Auschwitz inmate's notes from hell finally revealed, BBC, Dec. 1, 2017, available *at* https://www.bbc.com/news/world-europe-42144186 (last visited July 5, 2017); Brigit Katz, Reconstructed Auschwitz Letter Reveals Horrors Endured by Forced Laborer, SMITHSONIAN.COM, Oct. 11, 2017, available *at* https://www.smithsonianmag.com/smart-news/reconstructed-auschwitz-letter-reveals-horrors-endured-forced-laborer-180965238/ (last visited July 5, 2018).
27. Anita L. Allen, UNPOPULAR PRIVACY (2011), p. 22.
28. *See* the museum's statute, available *at* http://www.polin.pl/en/about-museum/public-private-partnership (last visited July 5, 2018). The museum is authorized to collect "databases providing scientific information, especially bibliographies, databases of historical addresses, address lists and name lists," among others.
29. Israel's Yad Vashem Law 1953, or the Act to Establish the United States Holocaust Memorial Council (HR 8081), passed by Congress in 1980.

are several lawful bases that may be relevant for such processing and publication. As mentioned in the opening of this article, Recital 158 makes specific reference to the Holocaust; though it is only partially coherent to this author, it does empower member states to legislate with regard to Holocaust archives—a power they have not yet exercised.

Finally, the legal argument made here, briefly, may form the basis for a joint position to be adopted by Holocaust research institutions, whose position would then be unified, consistent, and much simpler to promote and defend. There are several international bodies with a strong interest in supporting the work of Holocaust research institutions, any one of which could manage the joint position, and pooled resources, of these institutions in dealing with data protection. A centralized team charged with managing data protection for these institutions, including take-down requests, data subject access rights, data protection authority queries, and so on, would greatly improve their efficiency, and ease the risks associated with this crucial historical processing. Appended here is a draft proposal for such a joint position.

In conclusion, Holocaust researchers and institutions must work in unison to ensure that data protection protects the dignity and rights of the victims, and is not misused and abused to prevent justice and truth. The present article is hopefully a contribution to this united effort. ■

Arye Schreiber is a dual-qualified lawyer (England, Israel) specializing in data protection and privacy law. He is a Fellow of Information Privacy at the International Association of Privacy Professionals. Arye is founder and CEO of MyEDPO (www.myedpo.com), which acts as European Data Protection Officer for companies, government agencies, universities, and non-profits. He has published many articles on data protection law, and has lectured widely on data protection law and practice. Comments are welcome: arye@myedpo.com.

Appendix: Draft Holocaust Institution Joint Position on GDPR

This is a draft position to be taken by Holocaust research institutions (archives, museums, academic institutions, researchers, etc.) with regard to data protection law in Europe, and its applicability to Holocaust archives and research. It is presented here in the hope that the institutions, principally and presumably supported by one or more of the umbrella organizations, will consider formulating a joint position so as to enable Holocaust research, publication and education to continue to the greatest extent possible.

1. GDPR does not apply to data pertaining to the deceased (Recital 27). Overwhelmingly even survivors of the Holocaust are no longer alive. As such, unless it is proven otherwise, data pertaining to Holocaust victims and survivors are to be presumed to pertain to the deceased, and not to be within the scope of GDPR.
2. GDPR applies to "personal data," meaning "information relating to an identified or identifiable natural person" (Article 4(1)). Most Holocaust archival data cannot be tied to an identified or identifiable natural person, or that would require disproportionate resources.
3. Processing is a "legitimate interest" (Article 6(1)(f)) of Holocaust institutions, of victims and survivors and their families.
4. Processing is necessary for the performance of a task carried out in the public interest (Article 6(1)(e)).
5. Processing is necessary for the performance of a task carried out by law (Article 6(1)(c)). Institutions with an official state law mandate may sub-contract with other institutions to bring them within the relevant state law.
6. Holocaust institutions will support the passage of member state laws stipulating a duty to investigate and publish genocide and human rights abuses data (per Recital 158).
7. Holocaust institutions will establish a centralized team and body to manage their data protection risks and communications. They can also create a mutual indemnification or risk pool, to support each other in sharing the risk of data protection violations by their legitimate activities.
8. Specific rules can be drafted and followed to help categorize individual collections' data protection practices, and to govern given exceptional situations; for example, where a data subject is proven to be alive and to personally object to given processing, the institutions will endeavor to promptly cease that processing.
9. Holocaust institutions' reactions to data protection law will continue to serve as an example and precedent for investigations of other atrocities.