IT-PROJEKTMANAGEMENT BY DATENSCHUTZ-FOLGENABSCHÄTZUNG

Walter Hötzendorfer

Gemäß Art. 35 DSGVO ist in Bezug auf besonders risikogeneigte Formen der Verarbeitung personenbezogener Daten vorab eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Im vorliegenden Beitrag wird vorgeschlagen, anstatt die DSFA – wenn überhaupt – als nachgelagertes Teilprojekt eines Entwicklungsprojekts zu betrachten, den Prozess der Durchführung einer DSFA organisatorisch ins Zentrum der Entwicklung des gesamten Datenverarbeitungssystems zu stellen und das gesamte Entwicklungsprojekt aus dem DSFA-Prozess heraus zu managen, um auf diese Weise insbesondere den Informationsfluss und die Effizienz im Gesamtprojekt zu verbessern.

Inhaltsverzeichnis

1. EINLEITUNG

Es war und ist ein großes Anliegen und ein großes Talent von Friedrich Lachmayer, Menschen zusammenzubringen, Fachleute mit ihrer jeweiligen Expertise und ihren jeweiligen Handlungs- und Einflusssphären in produktiver Weise zu verknüpfen, um sie zu inspirieren und zu motivieren, Neues zu schaffen. Auch die Durchführung einer Datenschutz-Folgenabschätzung (DSFA) erfordert es, dass Menschen mit verschiedenen Expertisen und Zuständigkeiten zusammenwirken, um sich mit den Risiken einer geplanten Verarbeitung personenbezogener Daten und den Abhilfemaßnahmen zur Bewäl-

tigung dieser Risiken auseinanderzusetzen. Im Folgenden wird argumentiert, warum es sinnvoll ist, dass dieses Zusammenwirken nicht abgeschlossen in einem „DSFA-Projekt" erfolgt, sondern der Prozess der Durchführung einer DSFA organisatorisch ins Zentrum der Entwicklung des gesamten Datenverarbeitungssystems gestellt wird.

2. DAS INSTRUMENT DSFA

Eine DSFA ist ein Instrument zur Identifikation von Risiken und entsprechenden Abhilfemaßnahmen betreffend IT-Systeme zur Verarbeitung personenbezogener Daten. Art. 35 DSGVO verpflichtet für die Datenverarbeitung Verantwortliche in Bezug auf besonders risikoreiche Formen der Verarbeitung personenbezogener Daten, vorab eine DSFA durchzuführen, und normiert Vorgaben für die Durchführung. Die Durchführung einer DSFA kann in der Praxis sehr unterschiedlich ausfallen, eine DSFA hat jedoch gemäß Art. 35 Abs. 7 DSGVO jedenfalls eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, eine Bewertung der Notwendigkeit und der Verhältnismäßigkeit in Bezug auf den Zweck, eine Identifikation und Bewertung der Risiken sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen zu enthalten, woraus sich in gewisser Weise die Kernaufgaben der Durchführung einer DSFA ergeben.

In der Praxis besteht eine Tendenz, die DSFA erst spät im Entwicklungsprojekt und in Form eines mehr oder weniger isolierten Teilprojekts, wenn nicht überhaupt nur pro forma durchzuführen. Einer der wichtigsten Vorteile einer möglichst engen Integration der DSFA in den Entwicklungsprozess besteht darin, dass potenzielle Risiken frühzeitig identifiziert und geeignete Maßnahmen ergriffen werden können, um diese Risiken zu minimieren oder zu beseitigen. Wenn die DSFA erst durchgeführt wird, wenn das Datenverarbeitungssystem bereits entwickelt oder zumindest weit fortgeschritten ist, können potenzielle Risiken möglicherweise nicht mehr beseitigt werden oder erfordern erhebliche Änderungen am System, was zu Verzögerungen und erhöhten Kosten führen kann.

3. DIE DSFA ALS INSTRUMENT DES IT-PROJEKT-MANAGEMENTS

Über die offensichtlichen Vorteile im Sinne der Stärkung des Datenschutzes des zu entwickelnden Datenverarbeitungssystems hinaus ergeben sich auch für das Management

des gesamten Entwicklungsprojekts Vorteile, wenn die DSFA ins Zentrum des Projekts gestellt wird und als Management-Instrument verwendet wird. Dieser Vorschlag ist vor allem aufgrund der großen personellen und inhaltlichen Überschneidungen viel weniger gewagt, als er vielleicht zunächst erscheinen mag, und die Vorteile bestehen somit insbesondere im Nützen von Synergien und Vermeiden von Doppelgleisigkeiten, dem damit verbundenen sparsamen Umgang mit Personalressourcen und einem verbesserten Informationsaustausch, Wissens- und Anforderungsmanagement im Projekt.

Zunächst ist zu sagen, dass ohnehin für technische und organisatorische Entscheidungen im Entwicklungsprojekt und für die Durchführung der DSFA größtenteils dieselben handelnden Personen erforderlich sind: Einerseits müssen jene Personen, die das Gesamtsystem überblicken und beschreiben können, sowie Personen, die insbesondere aus technischer Sicht die Risiken beurteilen können, an der DSFA mitwirken, und andererseits ist umgekehrt auch die Involvierung von Datenschutzexpert:innen in das Entwicklungsprojekt erforderlich, wenn man die Verpflichtung zum Datenschutz durch Technikgestaltung (Art. 25 DSGVO) ernst nimmt.

Es ist daher zu empfehlen, dass es im Entwicklungsprojekt nur ein Team gibt, das sowohl dafür zuständig ist, das Projekt inhaltlich voranzutreiben, als auch dafür, die DSFA durchzuführen. Die bei der Durchführung der DSFA vor allem zum Zweck der Sachverhaltserhebung und später der Risikoanalyse erforderlichen Besprechungen bzw. Workshops sollen somit nicht separat durchgeführt werden, sondern wenn Festlegungen im Gesamtprojekt getroffen werden, soll dies gleich mit Blick auf den Datenschutz erfolgen und in der für den DSFA-Bericht erforderlichen Form dokumentiert werden. Insbesondere ist auch die Risikoanalyse, wie die gesamte DSFA, nicht bloß als Dokumentationsprojekt zur Erfüllung einer allfälligen Verpflichtung nach Art. 35 DSGVO zu verstehen, sondern ihre Ergebnisse müssen in das Entwicklungsprojekt zurückfließen und in der Gestaltung des Systems berücksichtigt werden.[1] Dies ist am besten dann möglich, wenn zwischen Projektteam und DSFA-Team bzw. zwischen Projektbesprechungen und DSFA-Besprechungen gar nicht erst unterschieden wird.

[1] Dies ergibt sich aus Art. 24, 25 und 32 DSGVO, insbesondere im Sinne der Verpflichtung zum Datenschutz durch Technikgestaltung.

Hinzu kommt, dass die DSFA wie erwähnt eine systematische Beschreibung des jeweils gegenständlichen Datenverarbeitungssystems erfordert. Im Zuge der Durchführung der DSFA müssen daher ohnehin viele Informationen über das zu entwickelnde System besprochen, von den Beteiligten verstanden und dokumentiert werden. Erfahrungsgemäß ist insbesondere dann, wenn eine DSFA in der gebotenen Ernsthaftigkeit und unter Einbeziehung externer Datenschutzexpert:innen durchgeführt wird, das Zusammenstellen einer systematischen Beschreibung der geplanten Verarbeitungsvorgänge – also aus juristischer Sicht die Beschreibung des Sachverhalts – ein sehr langwieriges Unterfangen. Häufig bedarf es zahlreicher Besprechungen mit Personen, die das Gesamtsystem überblicken und technisch beschreiben können, und zahlreicher Nachfragen bei bestimmten Projektbeteiligten, bis alle Informationen zum Sachverhalt vorliegen, die für die rechtliche sowie für die risikoorientierte Beurteilung erforderlich sind. Es ist dabei in der Praxis immer wieder festzustellen, dass bestimmte Fakten von durchaus zentraler Bedeutung entweder nur einer bestimmten Person im Projekt bekannt sind, nicht jedoch anderen davon betroffenen oder dafür eigentlich verantwortlichen Personen, oder sogar überhaupt noch nicht festgelegt wurden. Die aus der Perspektive des Datenschutzes erforderliche Akribie in Bezug darauf, wie genau ein bestimmter Aspekt ausgestaltet ist, im gesamten Projekt und von Anfang an walten zu lassen, kann somit Missverständnissen, Fehlentwicklungen und blinden Flecken vorbeugen, die ansonsten zu schwerwiegenden Problemen des zu entwickelnden Systems führen könnten.

Es ist darüber hinaus nicht sinnvoll, mehrere Systembeschreibungen oder -spezifikationen zu verfassen, sondern es ist zu empfehlen, eine einzige zu erstellen, die sich für den Zweck der DSFA ebenso eignet wie für andere Zwecke, für die eine solche erstellt wird, von der Spezifikation zwecks Schaffung eines gemeinsamen Verständnisses im Projekt bis hin zur Erläuterung des Systems Außenstehenden gegenüber. Diese Empfehlung verkennt nicht, dass viele IT-Systeme heute nicht mehr nach dem Wasserfallmodell entwickelt werden, an dessen Anfang eine Spezifikation steht, die sich in weiterer Folge nicht mehr ändern darf. Agile Softwareentwicklung und sich im Projektverlauf ändernde Anforderungen und Spezifikationen erschweren natürlich die Dokumentation des Systems, jedoch sind gerade diese Änderungen ein weiterer Grund, warum die Dokumentation und der Austausch darüber im Team wichtig sind, und schließlich muss ohnehin im DSFA-Bericht der der tatsächlichen Umsetzung entsprechende Letztstand dokumentiert sein. Erfahrungsgemäß führt somit gerade das DSFA-Erfordernis

einer systematischen Beschreibung der Verarbeitungsvorgänge tatsächlich auch dazu, dass es eine aktuelle Dokumentation des Systems gibt, die auch später vorgenommene Änderungen enthält.

Wenn man das alles betrachtet, wird deutlich, warum es nicht nur unzulässig, sondern vor allem auch ungeschickt wäre, die DSFA als Seitenprojekt links liegen zu lassen. Die Ergebnisse der DSFA müssen jedenfalls in die Entwicklung einfließen, und es bietet sich aus den genannten Gründen daher an, das Gesamtprojekt und die für die DSFA erforderlichen Schritte in einem gemeinsamen Team durchzuführen und insbesondere die DSFA-Dokumentation als zentrale Dokumentation des Gesamtprojekts zu führen.

4. ZUSAMMENFASSUNG UND AUSBLICK

Wie gezeigt wurde, kann es nicht nur für den Datenschutz des zu entwickelnden IT-Systems, sondern auch für das Management des gesamten Entwicklungsprojekts mehrere Vorteile haben, die DSFA ins Zentrum des Projekts zu stellen und als Management-Instrument zu benützen. Dieser Ansatz des IT-Projektmanagement by DSFA bedeutet konkret, dass DSFA-Team und Projektteam identisch sind, die Spezifikationen des zu entwickelnden Systems autoritativ als Sachverhaltsbeschreibung im DSFA-Bericht dokumentiert sind und nirgendwo sonst und sich ändernde Anforderungen und Spezifikationen dort nachgezogen werden. Diese Vorteile bestehen insbesondere in Synergien und im Vermeiden von Doppelgleisigkeiten, dem damit verbundenen sparsamen Umgang mit Personalressourcen und einem verbesserten Informationsaustausch, der geeignet ist, das Projekt vor ernsthaften Problemen zu bewahren.

Überwiegend können die erläuterten Vorteile auch erzielt werden, indem der Entwicklungsprozess und der DSFA-Prozess schlicht nicht mehr nebeneinander laufen, sondern die DSFA in das Projekt integriert wird. Die DSFA tatsächlich ins Zentrum des Entwicklungsprojekts zu setzen, manifestiert sich einerseits in einer Geisteshaltung, die dadurch in das gesamte Projekt ausstrahlt, und andererseits insbesondere darin, dass die DSFA-Dokumentation als zentrale Dokumentation des Gesamtprojekts geführt wird.

Zugegebenermaßen existiert der hier vorgeschlagene Ansatz bisher nur als Hypothese und wurde – soweit ersichtlich – noch nicht in die Tat umgesetzt. Ob dies in der

Praxis funktioniert, ob die genannten Vorteile auch eintreten und eventuell hier nicht vorhergesehene Nachteile dieses Ansatzes zutage treten, kann nur eine praktische Erprobung zeigen. Es wird mir hoffentlich gelingen, nicht zuletzt durch Verweis auf den vorliegenden Beitrag, ein Praxisprojekt nach dem hier vorgestellten Ansatz umzusetzen, also die DSFA wirklich ins Zentrum eines Entwicklungsprojekts zu stellen und als Instrument für das Management des gesamten Entwicklungsprojekts zu benützen. Genau dazu inspiriert uns Friedrich Lachmayers Wirken: sich zu trauen, einen Ansatz zu verwirklichen, der auf den ersten Blick vielleicht unkonventionell erscheinen mag, und Menschen mit ihren unterschiedlichen Fähigkeiten in bestmöglicher Weise zusammenwirken zu lassen.

Anmerkung:

Um aus dem vorliegenden Beitrag zugleich auch ein kleines Zeitdokument betreffend den aktuellen Stand der Entwicklung des maschinellen Lernens in seiner Rolle als Teilaspekt der Rechtsinformatik-Forschung zu machen, wurde im Laufe der Erstellung dieses Beitrags auch versucht, Teile davon mit Unterstützung von ChatGPT zu verfassen. Dies nicht, um den Aufwand zu reduzieren, sondern da das Thema des Beitrags in der Auseinandersetzung mit ChatGPT als besonders geeignet erschien, weil dessen Kernthese neu oder zumindest noch nicht breit diskutiert ist, und ein Large Language Model daher mutmaßlich nicht unmittelbar aus bereits existierenden Texten schöpfen kann, sondern tatsächlich eigenständig kreativ argumentieren müsste. Dies ist ChatGPT, konkret GPT-3.5 und GPT4, trotz mehrerer Versuche und mehrmaligem Nachfragen nicht gelungen. Es war in der Lage, eine schöne Einleitung zu verfassen und Vorteile des gegenständlichen Ansatzes für den Datenschutz zu erörtern, nicht jedoch, auch nicht auf direkte Nachfrage, zu argumentieren, warum dieser auch für das Management des Gesamtprojekts als solches von Vorteil sein kann. Lediglich aus Prinzip, um genau das einmal gemacht zu haben, wurde einer der generierten Absätze wörtlich in den Grundlagenteil des vorliegenden Beitrags übernommen.