Geschäftsplan für ein DIN SPEC-Projekt nach dem PAS-Verfahren zum Thema **„DIN SPEC Ein Prozess und Anforderungskatalog zur Überprüfung und Umsetzung der gesetzlichen Vorgaben im Umgang mit personenbezogenen Daten in KMU“**

Status:
Zur Kommentierung durch die Öffentlichkeit

Anmeldungen zur Mitarbeit sowie Kommentare zum Geschäftsplan sind erbeten und **bis zum 07.04.2020** an sobhi.mahmoud@din.de zu übermitteln[1]

Die Empfänger dieses Geschäftsplans werden gebeten, mit ihren Kommentaren **jegliche relevanten Patentrechte**, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Berlin, 09.03.2020 (Version 1)

[1] Anmeldungen zur Mitarbeit und Kommentare zum Geschäftsplan, die nach Ablauf der Frist eingehen, müssen nicht berücksichtigt werden. Über die Einarbeitung der fristgerecht eingegangenen Kommentare entscheidet das Konsortium (Gremium) nach seiner Konstituierung.

Inhaltsverzeichnis

1. Status/Version des Geschäftsplans

- **Zur Kommentierung durch die Öffentlichkeit (Version 1)**

  Dieser Geschäftsplan dient zur Information der Öffentlichkeit über das geplante Projekt. Interessenten haben die Möglichkeit, sich an dem Projekt zu beteiligen und/oder den Geschäftsplan zu kommentieren. Hierfür ist eine entsprechende E-Mail an sobhi.mahmoud@din.de zu richten.

  Über die tatsächliche Durchführung des Projekts entscheidet die Geschäftsleitung von DIN im Nachgang an die Veröffentlichung dieses Geschäftsplans.

  Kommt das Projekt zustande, werden alle Akteure, die sich fristgerecht zur Mitarbeit angemeldet oder den Geschäftsplan kommentiert haben, zum Kick-Off eingeladen.

- **Zur Erarbeitung der DIN SPEC (PAS) nach Annahme am <Datum Kick-off>**

  Änderungsvermerk zur Vorgängerversion xx:

  - z.B. Abschnitt 2: Tabelle der teilnehmenden Organisationen ergänzt
  - z.B. Abschnitt 7: Daten zum Konsortialleiter ergänzt
  - usw.

2. Initiator[2] und weitere Konsortialmitglieder

- Initiator:

Person/Organisation	Kurzbeschreibung
Sekina Mandelartz (Mandel VC GmbH)	Softwareanbieter für Datenschutz und informationssichere IT-Systeme.

[2] Die in diesem Dokument gewählte männliche Form der geschlechtsbezogenen Begriffe wie z. B. „der Initiator“ gelten selbstverständlich auch für alle weiblichen Personen. Lediglich aufgrund der besseren Verständlichkeit des Textes wurde einheitlich die männliche Form gewählt.

- Potenzielle zusätzliche Teilnehmer:

Die DIN SPEC wird durch einen Konsortium (temporäres Gremium) erarbeitet, der jedem Interessenten offen steht. Die Mitwirkung von weiteren Experten ist sinnvoll und wünschenswert. Es bietet sich an, dass sich beispielsweise

- Juristen
- IT-Beratungsunternehmen
- Datenschutzbeauftragte oder deren Verbände
- Repräsentanten von Verbraucherinteressen
- Forschungseinrichtungen
- Zertifizierungsstellen

an der Erarbeitung der DIN SPEC beteiligen.

- Organisationen[3], die sich zur Mitwirkung angemeldet haben:

Person	Organisation
Sekina Mandelartz	Mandel VC GmbH
Robert Blachnitz	Mandel VC GmbH
Prof. Dr. Marian Margraf	Freie Universität Berlin, Fraunhofer-Institut
Prof. Dr. Dominik Herrmann	Otto-Friedrich-Universität Bamberg
Sobhi Mahmoud	DIN

- Organisationen[3], die diesen Geschäftsplan angenommen haben (Konsortialmitglieder):

N.N.	N.N.
N.N.	N.N.
N.N.	N.N.

3. Ziele des Projekts

3.1. Allgemeines

Obwohl die EU-DSGVO bereits vor fast zwei Jahren in Kraft getreten ist und trotz drohender Bußgelder bei Datenpannen durch die Regulierungsbehörden, besteht in vielen Unternehmen in Deutschland immer noch eine mangelnde DSGVO-Konformität. Grund dafür dafür ist zum einen fehlende Transparenz in der Datenschutz(management)beratung und zum anderen mangelndes Wissen in der Umsetzung von Datenschutz gemäß EU-DSGVO. Zusätzlich besteht ein Nachfrageüberhang nach Expertenwissen im

Bereich der Datensicherheit, der mit einer überteuerten Datenschutzberatung einhergeht. Auch wenn (interne) Datenschutzbeauftragte bestellt wurden, herrscht aus Kundensicht das Gefühl von Überforderung und „Alleingelassen-Werden“ vor.

Das vielseitige Angebot an Beratungsleistungen, sowohl manuell als auch automatisiert, wird in unterschiedlicher Güte ausgeführt. Oft können Auftraggeber die Güte der Beratung nicht vollumfänglich abschätzen (Informationsasymmetrien), bis ein Kontakt mit Aufsichtsbehörden entsteht. Unternehmensberater agieren gern auf der Grundlage, ihre Beratungen frei von Normen und Standards zu gestalten, um einen Vergleich auszuschließen.

Die geplante Norm soll zu mehr Transparenz bei der Umsetzung der aus dem Datenschutzrecht resultierenden Anforderungen auf Basis einheitlicher Prozesse beitragen. Damit kann sie Organisationen unterschiedlicher Größen dabei unterstützen, Ressourcen einzusparen, Kosten zu senken und aus Sicht der Datenschutzaufsicht einen an Grundrechten orientierten Datenschutz durchzusetzen.

Das Basis-Datenschutz-Konzept (BDK) kann einerseits einen systematischen und nachvollziehbaren Vergleich zwischen Soll-Vorgaben, die sich aus Gesetzen und Verträgen ableiten, und andererseits die Umsetzung dieser Vorgaben sowohl auf organisatorischer als auch auf informationstechnischer Ebene bei der Verarbeitung personenbezogener Daten ermöglichen.

Ziel ist es, geeignete informationstechnische und organisatorische Mechanismen bereitzustellen, um Risiken, die mit der Verarbeitung personenbezogener Daten zwangsläufig einhergehen, beseitigen oder wenigstens auf ein tragbares Maß minimieren zu können.

Konkreter Nutzen zeichnet sich u.a. ab durch:

- Erhöhung der Effizienz

Das Optimierungspotenzial liegt in der Vereinfachung des IT-Alltags durch vorgefertigte Prozesse zum Datenschutz

- Mehr Transparenz durch klare Anforderungen

Einer nicht überschaubaren Anzahl an Beratungsleistungen zum Fachbereich Datenschutz kann mit unterschiedlichen Inhalten, Schwerpunkten, Vollständigkeit und Qualität durch klare Anforderungen an diese Dienstleistungen in Form eines Standards entgegengewirkt werden.

- Standardisierung von Datenschutzprozessen

Es bestünde die Möglichkeit zur Vorgabe und Standardisierung von Datenschutzprozessen zur Erreichung der Zertifizierungsreife gemäß EU-DSGVO. Es wäre eine “DAkkS (Deutsche Akkreditierungsstellen) - Zertifizierung” durch Stellen wie TÜV, DEKRA und andere akkreditierte Stellen möglich.

- Förderung der „Datenschutzreife“

Das Implementieren passender und relevanter Maßnahmen zur Datenschutzreife kann gefördert werden. Je nach Art der Organisation wirken Maßnahmen unterschiedlich in der Effektivität und Effizienz.

- Steigerung der Dokumentenqualität

Zur Steigerung der Qualität von Dokumenten können vorgefertigte Muster mit abgestimmten Regelungsinhalt zum Datenschutz übernommen werden.

- Kostenreduzierung

Es wäre eine Senkung der Kosten durch die Standardisierung der Datenschutzprozesse möglich. Positive Nebeneffekte könnten geringere Kosten bei den Versicherungspolicen sein.

- Einsparung von Ressourcen

Es findet eine Ressourceneffizienzsteigerung statt, da interne Mitarbeiter keine wissensbasierte Vorbereitung für Datenschutz benötigen, sondern ohne Expertenwissen durch den softwaregestützten Prozess geführt werden können.

- Standardisierter Datenschutzprozess

Jede Organisation erhält die Möglichkeit, etablierte bzw. standardisierte Datenschutzprozesse anzuwenden.

- Skalierung und Anerkennung von Expertenwissen

Das Skalieren von Expertenwissen durch softwareseitiges Fortschreiben der Prozesse hilft allen teilnehmenden Organisationen, Datenschutz besser umzusetzen. Zusätzlich kann mit einer Zertifizierung die fachliche Akzeptanz von Experten im Bereich Datenschutz gewürdigt und offiziell anerkannt werden.

- Bildung von Interessensgruppen

Kooperationen mit Verbänden und Interessensgruppen, beispielsweise dem Bundesverband Deutscher Startups, Bitkom, S.I.B.B. oder eco sind denkbar, um branchenspezifische Regelungen im Datenschutz fortzuschreiben.

- Abbau von Wissensgefällen

Durch das Auswählen und Definieren von Prozessen sowie Maßnahmen können unterschiedliche Wissensstände angeglichen und Datenschutz effektiver umgesetzt werden.

- Bereitstellung einer Anwendersicherheit

Es kann eine Anwendungssicherheit im Umgang mit Datenschutzvorgaben auch für Nicht-Experten gewährleistet werden.

3.2. Geplanter Anwendungsbereich

Der geplante Standard definiert einen Prozess und Anforderungskatalog, um die rechtlichen Anforderungen der EU-DSGVO zum Schutz personenbezogener Daten umzusetzen und in einem iterativen Prozess zu überprüfen und zu aktualisieren.

3.3. Verwandte Aktivitäten

Das Thema der geplanten DIN SPEC (PAS) ist bisher nicht Gegenstand einer Norm. Es existieren jedoch die folgenden, themenverwandten Gremien, Normen und/oder Regelwerke, die im Zuge des Projekts berücksichtigt und ggf. einbezogen werden:

- NA 043-01-27-05 AK - Identitätsmanagement und Datenschutz-Technologien
- DIN ISO/IEC 250xx Familie - Software Engineering - Qualitätskriterien und Bewertung von Softwareprodukten
- ISO 9126 - Qualitätsmerkmale für Software (Nachfolge-Norm ISO 25010)
- ISO 25010 - Qualitätsmerkmale für Software, zusätzlich mit Kategorie IT-Sicherheit und Kompatibilität
- ISO/IEC 270xx Familie - Informationssicherheit
- ISO/IEC 27001 (gemäß IT-Grundschutz) - Anforderungen an ein ISMS
- ISO/IEC 27018 - Security techniques - Code of practice for controls to protect personally identifiable information processed in public
- cloud computing services
- ISO/IEC 27031 - business continuity
- ISO/IEC 27032:2012 - Informationstechnologie – Sicherheitstechniken – Richtlinien für die Cybersicherheit
- ISO/IEC 27033 Revision
- ISO/IEC 27033-1 - Guidelines for network security
- ISO/IEC 27033-2 - Guidelines for the design and implementation of network
- ISO/IEC 27033-3 - Reference networking scenarios - Threats, design techniques and control issues
- ISO/IEC 27034 Guidelines for application security
- ISO/IEC 27552 (keine DSGVO-konforme Zertifizierungsnorm, eher Ergänzung um Datenschutzaspekte auf etwas
- Bestehendes gemäß ISO/IEC 27001)
- EN ISO 27799 Informationsicherheitsmanagement im Gesundheitswesen gemäß ISO/IEC 27002 IT-Sicherheitsverfahren
- ISO 9241 - Ergonomie der Mensch-System-Interaktion
- ISO/IEC/IEEE 29119 - Software Testing
- SDM - Standard-Datenschutzmodell der unabhängigen Datenschutzbehörden des Bundes und der Länder
- European Data Protection Board (edpb) - DSGVO: Leitlinien, Empfehlungen, bewährte Verfahren

4. Arbeitsprogramm

Im Zuge des Projekts soll eine DIN SPEC nach dem PAS-Verfahren (vgl. www.din.de/go/spec) erarbeitet werden. Die DIN SPEC darf nicht in Widerspruch zum Deutschen Normenwerk stehen.

Das Kick-Off wird voraussichtlich am 08.05.2020 in Berlin (DIN) stattfinden. Die Projektlaufzeit beträgt ca. 8 Monate.

Das Kick-Off dient der Konstituierung des Konsortiums, der Abstimmung bzw. Klärung weiterer organisatorischer Punkte sowie ggf. der Aufnahme der inhaltlichen Arbeiten.

Die Veröffentlichung eines Entwurfs zur Kommentierung durch die Öffentlichkeit ist nicht vorgesehen.

Insgesamt werden 2 Sitzungen (Kick off und Arbeitssitzungen) und 4 Webkonferenzen durchgeführt, um die jeweils bis dahin erarbeiteten Inhalte vorzustellen, abzustimmen und ggf. zu verabschieden. Die Erarbeitung der Inhalte kann durch einzelne Konsortialmitglieder oder Arbeitsgruppen erfolgen.

Die Terminierung der weiteren Projektmeetings und/oder Webkonferenzen erfolgt durch das Konsortium in Abstimmung mit DIN.

Die DIN SPEC wird in Deutsch erarbeitet (Sitzungssprache, Berichte, usw.). Die DIN SPEC wird in Deutsch verfasst.

ANMERKUNG In der Kalkulation wurde nur eine Sprachfassung berücksichtigt. Die Erarbeitung weiterer Sprachfassungen verursacht zusätzliche Kosten und muss deswegen gesondert vereinbart werden. Wenn eine weitere Sprachfassung gewünscht wird, kann die Übersetzung auch durch Beuth/DIN erfolgen. Diese wäre nach Verabschiedung des Manuskripts zur Veröffentlichung der DIN SPEC zusätzlich zu beauftragen.

5. Ressourcenplanung

Jedes Konsortialmitglied trägt seine im Rahmen des Vorhabens anfallenden Aufwendungen selbst.

Die Mitgliedschaft im Konsortium und die Teilnahme an den Projektmeetings ist kostenfrei, da die Kosten, die DIN aufgrund der Durchführung des Projekts entstehen, durch Mittel aus dem DIN-Connect-Projekt „Ein Prozess und Anforderungskatalog zur Überprüfung und Umsetzung der gesetzlichen Vorgaben im Umgang mit personenbezogenen Daten in KMU“ -gefördert durch DIN- finanziert werden.

6. Regeln der Zusammenarbeit im DIN SPEC (PAS)-Konsortium

Das Projekt unterliegt den PAS-Verfahrensregeln. Alle Interessenten und Konsortialmitglieder sind dazu aufgefordert, sich unter http://www.din.de/go/spec über die Verfahrensregeln in Kenntnis zu setzen.

Die Konstituierung des Konsortiums erfolgt im Zuge des Kick-Offs. Der Kick-Off findet erst statt, nachdem der Geschäftsplan veröffentlicht und die Durchführung des Projekts durch die DIN-Geschäftsleitung genehmigt wurde. Das Konsortium muss sich aus mindestens drei Konsortialmitgliedern unterschiedlicher Organisationen[3] zusammensetzen. Es ist nicht notwendig, dass diese unterschiedliche interessierte Kreise repräsentieren. Durch Zustimmung zum Geschäftsplan erklären die Interessenten ihre Bereitschaft zur Mitarbeit im Konsortium und werden dadurch formell zu Konsortialmitgliedern mit den einhergehenden Rechten und Pflichten. Teilnehmer des Kick-Offs, die den Geschäftsplan nicht annehmen, erhalten nicht den Status eines Konsortialmitglieds und sind von weiteren Entscheidungen des Kick-Offs sowie vom weiteren Projekt ausgeschlossen.

Entsendet eine Organisation (z. B. ein Verband) einen nicht-hauptamtlichen Mitarbeiter in das Konsortium, muss dieser von der Organisation autorisiert und DIN der Nachweis vorgelegt werden.

Jedes Konsortialmitglied erhält ein Stimmrecht und verfügt über jeweils eine Stimme. Entsendet eine Organisation mehrere Experten in das Konsortium, besitzt die Organisation, ungeachtet der Anzahl der entsendeten Teilnehmer, eine Stimme. Eine Übertragung von Stimmen auf andere Konsortialmitglieder ist nicht möglich. Bei Abstimmungen gilt einfache Mehrheit der abgegebenen Stimmen, wobei Stimmenthaltungen grundsätzlich nicht mitgezählt werden.

Das konstituierte Konsortium ist in der Regel geschlossen. Über die Aufnahme zusätzlicher Mitglieder entscheiden die bisherigen Konsortialmitglieder.

Im Zuge des Kick-Offs wählen die Konsortialmitglieder einen Konsortialleiter. Dieser leitet das Konsortium inhaltlich und führt die Entscheidungsfindung (Abstimmungen, Beschlüsse) herbei. Der Konsortialleiter wird hierbei durch den DIN-Projektmanager unterstützt, wobei DIN stets eine inhaltlich neutrale Position einnimmt. Darüber hinaus trägt der DIN-Projektmanager dafür Sorge, dass die Verfahrens- und Gestaltungsregeln von DIN bei der Erstellung der DIN SPEC eingehalten werden. Sollte der Konsortialleiter seine Funktion nicht mehr wahrnehmen können, werden vom DIN-Projektmanager Neuwahlen initiiert.

[3] Organisationen sind teilnehmende juristische Personen, die die Experten in das DIN SPEC PAS-Konsortium entsenden und einer Unternehmensstruktur i.S.v. § 15 Aktiengesetz oder § 271 Absatz 2 Handelsgesetzbuch zuzurechnen sind.

Die Organisation und Leitung des Kick-Offs erfolgt durch den DIN-Projektmanager in Abstimmung mit dem Initiator. Die übrigen Projektmeetings und/oder Webkonferenzen werden vom DIN-Projektmanager in Abstimmung mit dem Konsortialleiter organisiert.

Wenn Konsortialmitglieder bei der Verabschiedung der DIN SPEC bzw. des Entwurfs nicht anwesend sein können, sind diese über alternative Wege (z. B. schriftlich, elektronisch) in die Abstimmung einzubeziehen.

Alle Konsortialmitglieder, die für die Veröffentlichung der DIN SPEC bzw. des Entwurfs gestimmt haben, werden als Verfasser namentlich und mit der zugehörigen Organisation im Vorwort aufgeführt. Alle Konsortialmitglieder, die gegen die Veröffentlichung der DIN SPEC bzw. des Entwurfs gestimmt oder sich enthalten haben, dürfen nicht im Vorwort genannt werden.

Über eine nachträgliche Erweiterung des Konsortiums entscheiden die bisherigen Konsortialmitglieder. Dabei ist insbesondere zu berücksichtigen, dass

a) die Erweiterung förderlich ist, die Projektdauer zu verkürzen bzw. ein drohender Verzug der geplanten Projektdauer vermieden bzw. abgewendet werden kann;
b) die Erweiterung nicht zu einer drohenden Verlängerung der Projektdauer führt;
c) das neue Konsortialmitglied keine neuen oder ergänzenden Sachverhalte abseits des im Geschäftsplans festgelegten und bewilligten Anwendungsbereiches thematisiert;
d) das neue Konsortialmitglied ergänzendes Fachwissen mitbringt, damit die neuesten Erkenntnisse der Wissenschaft und der jeweilige Stand der Technik eingebracht werden;
e) das neue Konsortialmitglied sich aktiv an der Manuskriptarbeit beteiligt durch Einbringen konkreter, aber nicht abstrakter Vorschläge und Beiträge.
f) das neue Konsortialmitglied für eine verstärkte Anwendung der DIN SPEC (PAS) sorgt.

Um die sachgerechte Vervielfältigung und Verbreitung der Ergebnisse der Standardisierungsarbeit zu ermöglichen, räumen die Konsortialmitglieder DIN die Nutzungsrechte an den ihnen erwachsenden Urheberrechten an den Ergebnissen der Standardisierungsarbeit ein. Die Einräumung der Urhebernutzungsrechte hindert die Mitglieder des Konsortiums nicht daran, ihr eingebrachtes Wissen, ihre Erfahrungen und Erkenntnisse weiterhin zu nutzen, zu verwerten und weiterzuentwickeln.

Die Konsortialmitglieder sind angehalten, DIN über relevante Patentrechte, die in Zusammenhang mit diesem DIN SPEC Projekt stehen, zu informieren.

Nachträgliche Änderungen am Anwendungsbereich (Abschnitt 3.2) oder an der Ressourcenplanung (Abschnitt 6) erfordern neben einer 2/3-Mehrheit aller abgegebenen Stimmen zusätzlich die Zustimmung von DIN.

7. Kontaktpersonen

- Konsortialleiter:
  N.N.

- Projektmanager:
  Sobhi Mahmoud
  DIN Deutsches Institut für Normung e. V.
  Saatwinkler Damm 42/43
  13627 Berlin
  Tel.: + 49 30 2601- 2061
  Fax: + 49 30 2601 - 42061
  E-Mail: sobhi.mahmoud@din.de

- Initiator:
  Sekina Mandelartz
  Mandel VC GmbH
  Bennigsenstraße 27
  12159 Berlin
  Tel.: + 49 157 71 91 8874
  s.mandelartz@audat.de

Anhang: Zeitplan (vorläufig)

DIN SPEC-Projekt	2020																							
	Jan		Feb		Mrz		Apr		Mai		Jun		Jul		Aug		Sep		Okt		Nov		Dez	
Initiierung																								
1. Antrag und Prüfung																								
2. Erstellung des Geschäftsplans																								
3. Veröffentlichung des Geschäftsplans																								
Workshop-Phase																								
4. Kick-Off / Konstituierung des Konsortiums																								
5. Erstellung der DIN SPEC (PAS)																								
6. Verabschiedung DIN SPEC (PAS) im Konsortium																								
Veröffentlichung																								
7. Prüfung und Freigabe durch DIN																								
8. Veröffentlichung der DIN SPEC (PAS)																								
Meilensteine									**K**		**W**		**W**			**W**		**M**			**W / V**			

K Kick-Off
M Projektmeeting
W Webkonferenz
V Verabschiedung der DIN SPEC (PAS)