Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
I. Data Protection by Design				
I.1 Können einzelne Datensätze mit personenbezogenen Daten individuell gelöscht werden?	Es muss gewährleistet sein, dass Datensätze individuell löschbar sind. So können Betroffenenbegehren (insb. Art. 17 DSGVO) angemessen umgesetzt werden. Idealerweise sind Datensätze nicht nur vollständig, sondern auch partiell löschbar.	Ja ☒ Nein ☐	Personenbezogene Daten (Name, Wohnort, Geb.tag, etc.) können in der Anwendung direkt gelöscht bzw. geändert werden. Benutzerkonten können vollständig gelöscht werden (ab Version 5.0.2.0).	Datenminimierung DSFA Kapitel 6.5
I.2 Ist die Sperrung einzelner Datensätze möglich?	Um das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) zu wahren, müssen Datensätze für die weitere Verarbeitung gesperrt werden können. Dabei ist zu beachten, dass die Sperrung reversibel sein muss, damit Rechte angemessen gewahrt werden können.	Ja ☐ Nein ☒	Es findet nur ein begrenzter Einsatz von personenbez. Daten zu den umsatzlosen Sparkonten statt. Eine vorübergehende Sperrung von Datensätzen und demnach der Konten ist für die Anwendung nicht zweckmäßig.	Datenminimierung DSFA Kapitel 6.5
I.3 Ist die Zahl der Eingabefelder auf das Wesentliche begrenzt?	Gemäß dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Daraus folgt, dass in einem System nur die Eingabefelder vorhanden sein sollten, deren Daten für die konkrete Verarbeitung benötigt	Ja ☒ Nein ☐	Mussfelder beim Import von Kontodaten: Name, Ort, PLZ Benutzer: weder Vor- noch Nachname bei	Datenminimierung DSFA Kapitel 6.5

Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
	werden. Auf diese Weise soll eine Vorratsdatenspeicherung verhindert werden. Zudem sollte die Anzahl an Freitextfeldern auf das Notwendige minimiert werden. In Freitextfeldern werden des Öfteren persönliche Anmerkungen der Sachbearbeiter notiert, deren Inhalte im Falle der Bereitstellung einer Kopie im Rahmen der Betroffenenauskunft nach Art. 15 DSGVO auch negative Auswirkungen auf die Geschäftsbeziehung nach sich ziehen können.		Anlegen notwendig (S-Kennung reicht aus)	
I.4 Sind Einwilligungen des Betroffenen dokumentierbar?	Falls personenbezogenen Daten über den ursprünglichen Zweck hinaus oder für Direktwerbung verwendet werden sollen, ist eine Einwilligung des Betroffenen einzuholen. Diese Einwilligung ist zu dokumentieren.	Ja ☐ Nein ☒	Nicht relevant, da ausschließlich Daten von bestehenden Konten (aufgelöste Konten siehe II.8) bzw. Benutzerinformationen verarbeitet werden. Ggf. können Einträge in das Notizfeld vorgenommen werden.	Transparenz DSFA Kapitel 6.6 Intervenierbarkeit DSFA Kapitel 6.8
I.5 Ist sichergestellt, dass bei fehlender bzw. widerrufener Einwilligung eine über den ursprünglichen Zweck hinausgehende Datenverarbeitung bzw. Direktwerbung nicht länger möglich sind?	Sofern die Einwilligung des Betroffenen widerrufen wird (bzw. gar nicht erst bestand), dürfen Datenverarbeitungen, die über den ursprünglichen Zweck der Datenerhebung hinausgehen, nicht (weiter) durchgeführt werden. Dies gilt insbesondere für die direkte Bewerbung des Kunden via Telefon oder elektronischer Medien.	Ja ☐ Nein ☒	Nicht relevant, da ausschließlich Daten von bestehenden Konten (aufgelöste Konten siehe II.8) bzw. Benutzerinformationen verarbeitet werden.	Nichtverkettung DSFA Kapitel 6.7

Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
I.6 Ist sichergestellt, dass nur der für die Erfüllung der Datenverarbeitung notwendige Personenkreis Zugriff auf die personenbezogenen Daten erhält?	Im Rahmen der technischen und organisatorischen Maßnahmen muss durch ein entsprechendes Rechte- und Rollenkonzept sichergestellt sein, dass nur die Mitarbeiter, die tatsächlich personenbezogene Daten verarbeiten müssen, Zugriff auf diese Daten erhalten. Zu umfangreiche Zugriffsrechte erhöhen das Risiko, dass Daten ohne Rechtsgrundlage oder für nicht legitime Zwecke verarbeitet werden könnten.	Ja ☒ Nein ☐	Benutzerverwaltung: Benutzer erhält ausschließlich die definierten Berechtigungen seiner/ihrer Rolle über Windows-Login (S-Kennung).	Vertraulichkeit DSFA Kapitel 6.1
I.7 Sind Möglichkeiten zur Erfüllung von Betroffenenanfragen gegeben?	Neben den Rechten zur Löschung bzw. Einschränkung der Bearbeitung (s.o.) sind insbesondere folgende Rechte von größerer Relevanz: • Recht aus Auskunft, Art. 15 DSGVO • Recht auf Berichtigung, Art. 16 DSGVO • Recht auf Datenübertragbarkeit, Art. 20 DSGVO • Widerspruchsrecht, Art. 21 DSGVO Es soll sichergestellt sein, dass über das System diese Rechte gewahrt werden können. Eine Auskunft aller relevanten personenbezogenen Daten sollte neben der einfachen Erstellung einer Kopie dieser Daten in einem lesbaren Format möglich sein. Personenbezogene Daten sollen von berechtigten Mitarbeitern einfach aber nachvollziehbar berichtigt werden können. Ein Datenexport in einem maschinenlesbaren Format sollte ebenso möglich sein wie eine Sperrung der Verarbeitung nach erfolgtem Widerspruch.	Ja ☒ Nein ☐	Personensuche möglich, Korrektur von Personendaten über Konto bearbeiten.	Transparenz DSFA Kapitel 6.6
I.8 Sind sichere Schnittstellen zur Datenübermittlung vorhanden?	Sofern ein Datenaustausch zwischen dem System und weiteren Systemen gewünscht ist, sollten kompatible Schnittstellen zwischen diesen Systemen vorliegen. Dies soll sicherstellen, dass die personenbezogenen Daten unverfälscht zwischen den Systemen ausgetauscht werden	Ja ☐ Nein ☒	Nicht relevant. Sparbuch UL hat keine (direkte) Schnittstellen zu anderen Anwendungen,	Integrität DSFA Kapitel 6.2 Vertraulichkeit

Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
	können. Solche Schnittstellen sind allerdings erfahrungsgemäß Angriffspunkte für externe Angreifer. Aus diesem Grund sollten die Schnittstellen derart abgesichert sein, dass ein Datenaustausch nur mit (z.B. über digitale Signaturen) legitimierten Systemen möglich ist und eine dem Schutzbedarf der Daten entsprechende Verschlüsselung des Transportwegs erfolgt.		Internet oder E-Mail-Versand.	DSFA Kapitel 6.1
I.9 Können über die Schnittstellen auch Informationen zur Erfüllung von Betroffenenanfragen weitergegeben werden?	Selbst bei Verwendung eines zentralen Kernbankensystems sind verschiedene personenbezogene Daten oftmals dezentral in unterschiedlichen Systemen gespeichert. Um die Wahrung von Betroffenenrechten hinreichend zu gewährleisten, sollten auch im Rahmen von Betroffenenanfragen personenbezogene Daten aus anderen Systemen abgerufen oder an die relevanten Systeme übermittelt werden können.	Ja ☐ Nein ☒	Nicht relevant. Sparbuch UL hat keine (direkte) Schnittstellen zu anderen Anwendungen, Internet oder E-Mail-Versand.	Intervenierbarkeit DSFA Kapitel 6.8 Transparenz DSFA Kapitel 6.6
I.10 Ist die Einhaltung der Grundsatzes des Datenschutzes durch Technikgestaltung vom Hersteller nachweisbar?	Eine Überprüfung der Einhaltung der Grundsätze des Art. 25 DSGVO ist durch den Endanwender in der Regel unmöglich. Um dennoch eine Nachweisbarkeit herstellen zu können, sollte es alternativ ausreichen, wenn der Hersteller die Datenschutzkonformität durch sonstige Nachweise belegen kann. Ein solcher Nachweis kann durch ein anerkanntes Prüfsiegel oder anhand von anerkannten Auditberichten erfolgen.	Ja ☒ Nein ☐	Nachweis ist dieses Dokument.	Stand der Technik

Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
I.11 Sind alle Änderungen an Datensätzen nachvollziehbar?	Änderungen an personenbezogenen Daten sollten mit Zeitstempel und Bearbeiterkürzel protokolliert werden, um Manipulationen nachweisen zu können.	Ja ☒ Nein ☐	Veränderungen an Kontodaten werden geloggt (inkl. Kontonummer und Benutzer).	Transparenz DSFA Kapitel 6.6
I.12 Werden personenbezogene Daten sicher gespeichert?	Systemrelevante Datenbanken, welche personenbezogene Daten enthalten, sollten mit einem aktuell als sicher anerkannten Algorithmus verschlüsselt werden, um das Risiko eines unberechtigten Zugriffs auf Daten zu verringern.	Ja ☐ Nein ☒	Nicht anwendbar, da institutseigene Datenbank. Ein direkter Zugang auf Datenbank ist nur durch DB-Administratoren möglich.	Vertraulichkeit DSFA Kapitel 6.1
II. Data Protection by Default				
II.1 Sind keine vorab verfügbaren Freitextfelder vorhanden?	Es sollten per Voreinstellung keine offenen Freitextfelder vorhanden sein. Sofern Freitextfelder erforderlich sein sollten, sollten diese durch gesondert berechtigte Mitarbeiter und auch nur für den konkreten Anlass freigeschaltet werden können.	Ja ☐ Nein ☒	In Sparbuch UL existiert nur ein einziges Freitextfeld (Notiz), welches keiner separaten Berechtigung unterliegt.	Datenminimierung DSFA Kapitel 6.5
II.2 Ist sichergestellt, dass das System keine Daten an den Hersteller bzw.	Zur Prüfung der Stabilität und Leistungsfähigkeit und zur Durchführung von Supportaufgaben übermitteln verschiedene Systeme dauerhaft personenbezogene Daten	Ja ☒ Nein ☐	Sowohl Anwendung als auch Datenbank liegen auf institutseigenen	Nichtverkettung DSFA Kapitel 6.7

Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
den Wartungsdienstleister übermittelt?	wie IP-Adresse oder Benutzerkennungen an den Systemhersteller oder einen beauftragten Wartungsdienstleister. Diese Übermittlungen erfolgen oftmals intransparent für den Endanwender und ohne explizite Rechtsgrundlage. Aus diesem Grund sollte sichergestellt sein, dass solche für die Telemetrie relevanten Daten nur dann an den Hersteller oder einen Wartungsdienstleister übermittelt werden, wenn dies von Seiten des Anwenders bzw. eines Mitarbeiters aus der hauseigenen IT-Abteilung genehmigt worden ist.		SIA-Servern. Es erfolgt keine (automatisierte) Übermittlung von Daten an den Dienstleister.	
II.3 Ist sichergestellt, dass Remotezugriffe nur anlassbezogen erfolgen können?	Remotezugriffe auf das System sollten nur durch eine aktive Zustimmung des Users möglich sein und dürfen nur so lange aufrechterhalten werden, wie dies für die Remotetätigkeit erforderlich ist. Wird die Verbindung geplant oder ungeplant unterbrochen, sollte eine erneute Zustimmung des Users zum Remotezugriff erforderlich sein.	Ja ☒ Nein ☐	Ein direkter Remotezugriff ist nicht möglich und kann ggf. nur über andere Programme (z.B. Skype) von außerhalb des Instituts erfolgen.	Nichtverkettung DSFA Kapitel 6.7
II.4 Ist sichergestellt, dass Datenübermittlungen nur erfolgen, wenn der User aktiv zugestimmt hat?	Übermittlungen personenbezogener Daten an andere Stellen sind nur unter Vorliegen einer Rechtsgrundlage und eines legitimen Zwecks zulässig. Um sicherzustellen, dass Daten nicht permanent übermittelt werden oder von anderen Systemen abgerufen werden können, sollten Datenübermittlungen nur aktiv durch den User oder einen berechtigten Mitarbeiter angestoßen werden können. Dabei ist es unerheblich, ob es sich um eine einmalige Datenübermittlung oder über eine geplante regelmäßige Datenübermittlung handelt.	Ja ☒ Nein ☐	Eine Übermittlung von Daten nach außen kann nur mittels andere Programme/Systeme durch den User erfolgen (z.B. SecureMail).	Nichtverkettung DSFA Kapitel 6.7

Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
II.5 Ist sichergestellt, dass User nur die Benutzerrechte haben, welche sie für ihre Tätigkeit benötigen?	Das Rechte- und Rollenkonzept sollte gewährleisten, dass höherrangige Benutzerrechte nur einem kleinen Personenkreis vorbehalten bleiben (Need-to-know-Prinzip).	Ja ☒ Nein ☐	Integrierte Benutzerverwaltung mit Definition von entsprechenden Rollen.	Vertraulichkeit DSFA Kapitel 6.1
II.6 Ist sichergestellt, dass bei der Verarbeitung besonders sensitiver Daten höhere Umsicht gewahrt wird?	Bei der Verarbeitung besonders schützenswerter Daten sollte darauf geachtet werden, dass diese Verarbeitung höhere Sicherheitsstandards erfüllt als bei weniger schützenswerten Daten. Dies kann bspw. durch die technische oder organisatorische Umsetzung eines Vier-Augen-Prinzips gewahrt werden.	Ja ☒ Nein ☐	Für verschiedene Funktionen ist ein 4-Augenprinzip aktivierbar (Jahreszinslauf, Benutzergruppen, Einstellungen)	Vertraulichkeit DSFA Kapitel 6.1
II.7 Ist sichergestellt, dass nur berechtigte Personen mit dem System arbeiten können?	Benutzerkonten sollen personengebunden sein und eine Mehrfaktorautorisierung (z.B. durch Benutzername und Passwort) benötigen, damit sichergestellt ist, dass nur berechtigte Personen Daten verarbeiten können.	Ja ☒ Nein ☐	Zugriff auf Anwendung nur über KURS-Berechtigung. Start der Anwendung nur möglich, wenn der Benutzer in der Anwendung selbst angelegt ist.	Vertraulichkeit DSFA Kapitel 6.1
II.8 Ist die Löschung von personenbezogenen Daten gewährleistet?	Personenbezogene Daten und Belegen sollten nach Ablauf einer festgelegten Löschfrist automatisch gelöscht werden. Ausnahmen von dieser automatisierten Löschung dürfen nur durch berechtigte Benutzer gesondert definiert werden.	Ja ☒ Nein ☐	Aufgelöste Konten werden nach einer parametrisierten Zeitdauer anonymisiert.	Datenminimierung DSFA Kapitel 6.5

Frage	Erläuterung	Vorhanden?	Bei 'Ja': Beschreibung der Maßnahme und Dokumentation, bei 'Nein': Begründung	Gewährleistungs-ziele gemäß SDM
II.9 Ist sichergestellt, dass die Verarbeitung von personenbezogenen Daten an eine Rechtsgrundlage gebunden ist?	Bestimmte Funktionen der Datenverarbeitungen dürfen nur durchgeführt werden, wenn eine explizite Rechtsgrundlage zur Datenverarbeitung (z.B. in Form einer Kundeneinwilligung) gegeben ist. Ansonsten sind die entsprechenden Datensätze für diese Funktionen gesperrt und können auch im Rahmen von Stapelverarbeitung nicht verwendet werden.	Ja ☒ Nein ☐	Es werden nur die gesetzlich notwendigen Personendaten von bestehenden Konten verarbeitet. Informationen von aufgelösten (ausgezahlten) Konten werden nach einer bestehenden Aufbewahrungspflicht anonymisiert.	Nichtverkettung DSFA Kapitel 6.7
II.10 Ist die Einhaltung der Grundsatzes des Datenschutzes durch datenschutzfreundliche Voreinstellungen vom Hersteller nachweisbar?	Eine Überprüfung der Einhaltung der Grundsätze des Art. 25 DSGVO ist durch den Endanwender in der Regel unmöglich. Um dennoch eine Nachweisbarkeit herstellen zu können, sollte es alternativ ausreichen, wenn der Hersteller die Datenschutzkonformität durch sonstige Nachweise belegen kann. Ein solcher Nachweis kann durch ein anerkanntes Prüfsiegel oder anhand von anerkannten Auditberichten erfolgen.	Ja ☒ Nein ☐	Nachweis ist dieses Dokument.	Stand der Technik