Bayerisches Landesamt für
Datenschutzaufsicht

Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.

Muster 8: Genossenschaftsbank

Hinweis:
Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist ein sog. *Verantwortlicher*. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen der DS-GVO einhält. In der folgenden Übersicht werden die *wesentlichen* Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesem Muster wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den jeweiligen Anforderungen sind auf der Rückseite dieses Papiers zu finden.

Kurzbeschreibung der Genossenschaftsbank

Eine Bank hat 60 Beschäftigte, welche die Bankgeschäfte mit Verbrauchern, Firmen, Selbständigen, Vereinen usw. betreuen. Fünf dieser Beschäftigten sind für die IT, drei für die Personalverwaltung sowie zwei im Werbebereich tätig. Hinzu kommen zwei Reinigungskräfte und ein Hausmeister. Auf Grund des Sicherheitsbereichs wird im Kassenbereich und an den Geldautomaten Videoüberwachung praktiziert.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Verarbeitung der Daten zu den Bankgeschäften, auch unter Einschaltung eines externen Rechenzentrums
- Lohnabrechnung der eigenen Beschäftigten
- Scoring-Verfahren zur kundenindividuellen Bonitätsbewertung
- Betrieb einer Website für Online-Kontoführung
- Videoüberwachung der Kasse und der Geldautomaten

Wesentliche DS-GVO-Anforderungen für die Genossenschaftsbank

A Datenschutzbeauftragter (DSB)
Muss ein DSB vom der Bank benannt werden?
☒ ja (mindestens 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)
☐ nein

B Verzeichnis von Verarbeitungstätigkeiten
Ist ein solches Verzeichnis erforderlich?
☒ ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
☐ nein

C Datenschutz-Verpflichtung von Beschäftigten
Ist eine solche Verpflichtung durchzuführen?
☒ ja (für alle Mitarbeiter, die mit personenbezogenen Daten umgehen)
☐ nein

D Information- und Auskunftspflichten
Bestehen irgendwelche Informationspflichten?
☒ ja (bei den Beschäftigten und Kunden sowie auf der Webseite in der Datenschutzerklärung)
☐ nein

E Löschen von Daten
Gibt es eine Anforderung zur Datenlöschung?
☒ ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
☐ nein

F Sicherheit
Müssen die Daten besonders gesichert werden?
☒ ja (neben den Standardmaßnahmen sind weitere Sicherheitsmaßnahmen erforderlich)
☐ nein

G Auftragsverarbeitung
Ist ein Vertrag zur Auftragsverarbeitung notwendig?
☒ ja (sowohl mit dem Hosting-Anbieter für die Website als auch mit dem externen Rechenzentrum)
☐ nein

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
☒ ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
☐ nein

I Datenschutz-Folgeabschätzung (DSFA)
Muss eine DSFA vom Verein durchgeführt werden?
☒ ja (beim Scoring-Verfahren könnte ein hohes Risiko bestehen und somit eine DSFA erforderlich sein)
☐ nein

J Videoüberwachung (VÜ)
Besteht eine Ausschilderungspflicht bezüglich VÜ?
☒ ja (im Kassen und Automatenbereich ist u.a. eine entsprechende Ausschilderung notwendig)
☐ nein

ⓘ Erläuterungen zu den Anforderungen

A Datenschutzbeauftragter (DSB)

Ein DSB ist zu benennen, wenn *mindestens 10 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. „Ständig beschäftigt" ist, wer z. B. täglich laufend mit personenbezogenen Daten arbeiten muss. „Nicht ständig beschäftigt" damit ist dagegen z. B., wer nur Reinigungs- oder Hausmeisterarbeiten durchführt und dabei Papierabfall entsorgt.

⇨ **DSK-Kurzpapier Nr. 12:** *www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf*

B Verzeichnis von Verarbeitungstätigkeiten

Unternehmen müssen für ihre Verwaltungstätigkeiten, die (auch) personenbezogene Daten betreffen, ein – vom Umfang her sehr überschaubares – Verzeichnis ihrer Verarbeitungstätigkeiten führen.

⇨ **DSK-Kurzpapier Nr. 1:** *www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf*
⇨ **DSK-Muster-Verzeichnis allgemein:** *www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf*

C Datenschutz-Verpflichtung von Beschäftigten

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt.

⇨ **DSK-Kurzpapier Nr. 19:** *https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_19.pdf*

D Informations- und Auskunftspflichten

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Zumindest muss er darauf hinweisen, wo die Informationen leicht zugänglich sind (z. B. Informationsblatt, Homepage). Die betroffenen Personen haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten

⇨ **DSK-Kurzpapier Nr. 6:** *www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf*
⇨ **DSK-Kurzpapier Nr. 10:** *www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf*

E Löschen von Daten

Sobald keine gesetzliche Grundlage (z. B. steuerliche Aufbewahrungspflicht) mehr für die Speicherung von personenbezogenen Daten mehr besteht, sind diese zu löschen. In der Regel ist dies bspw. nach zehn Jahren der Fall.

⇨ **DSK-Kurzpapier Nr. 11:** *www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf*

F Sicherheit

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind nicht nur Standardmaßnahmen erforderlich. Hinzu kommen u. a. die bankspezifischen Anforderungen, siehe z. B. die „Bankaufsichtlichen Anforderungen an die IT" von der BaFin.

⇨ **BayLDA-Kurzpapier Nr. 1:** *www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf*

G Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. IT-Arbeiten oder Website-Hosting) an Externe auslagern, um personenbezogene Daten in ihrem Auftrag durch andere verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.

⇨ **DSK-Kurzpapier Nr. 13:** *www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf*
⇨ **BayLDA-Formulierungshilfe zum Vertrag:** *www.lda.bayern.de/media/muster_adv.pdf*

H Datenschutzverletzungen

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Kunden- oder Beschäftigtendaten), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

⇨ **BayLDA-Kurzpapier Nr. 8:** *www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf*
⇨ **BayLDA-Online-Service zur Meldung:** *www.lda.bayern.de/de/datenpanne.html*

I Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist der Ausnahmefall, aber bei Scoringverfahren anzunehmen.

⇨ **DSK-Kurzpapier Nr. 5:** *www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf*

J Videoüberwachung

Führt ein Verantwortlicher eine Videoüberwachung durch, ist eine entsprechende Hinweisbeschilderung erforderlich, um die betroffenen Personen über die Videoaufnahmen zu informieren.

⇨ **DSK-Kurzpapier Nr. 15:** *www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf*