Informationen für Maßnahmeträger zum Umgang mit (elektronischen) Unterschriften/Signaturen in Maßnahmen zur Aktivierung und beruflichen Eingliederung nach § 45 SGB III

Aufgrund verschiedener Anfragen von Maßnahmeträgern möchten wir zu diesem Thema informieren. Insbesondere geht es um **Anwesenheitslisten für die Teilnahme an zugelassenen Maßnahmen mittels eines Aktivierungs- und Vermittlungsgutscheins für Maßnahmen bei einem Träger (AVGS MAT)**.

Die nachfolgenden Ausführungen beziehen sich zunächst nur auf **Maßnahmen zur Aktivierung und beruflichen Eingliederung** sowohl aus dem Rechtskreis SGB III als auch aus dem Rechtskreis SGB II.

Maßnahmeträger werden in der Mitteilung über die Bewilligung einer Teilnahme darauf hingewiesen, mit jeder Rechnung die zugehörige **Anwesenheitsliste** einzuschicken, aus der die **pro Tag bzw. pro Termin absolvierte Zahl an Maßnahmestunden** hervorgeht. Die Maßnahmestunden sind durch die teilnehmende Person für jeden Tag bzw. jeden Termin separat zu bestätigen. Dies kann handschriftlich oder mittels digitaler Unterschrift erfolgen. Dies gilt für alle Durchführungsformen (Präsenz, hybrid oder ausschließlich digital/online).

Für die Verwendung eines eigenen digitalen Unterschrifts- und Teilnahmekontrollsystems benötigt ein Maßnahmeträger **keine vorherige Genehmigung** oder Freigabe.

Bei **Nutzung einer digitalen Unterschrift** durch die teilnehmende Person zur Bestätigung der absolvierten Maßnahmestunde/n bzw. des absolvierten Tages / Termins ist wesentliches Kriterium, dass diese **manipulationssicher** sein muss. Es darf nicht möglich sein, dass eine einmal geleistete Unterschrift ohne Wissen der Person kopiert und erneut genutzt wird. Weiterhin muss nachvollziehbar sein, dass die teilnehmende Person die Unterschrift jedes Mal selbst geleistet hat. Es darf kein Automatismus dahinterliegen. Die teilnehmende Person muss jedes Mal die elektronische Unterschrift bewusst und aktiv leisten.

Eine digitale Unterschrift wird daher nur akzeptiert, wenn ein **digitales Zertifikat** oder bei einzelnen unterschriebenen Dokumenten ein sogenanntes **Prüfprotokoll** beigefügt wird. Es muss ersichtlich sein, zu welchem Zeitpunkt die digitale Unterschrift durch die teilnehmende Person vorgenommen wurde. Ersatzweise wird auch ein Zeitstempel bei der digitalen Unterschrift akzeptiert, aus dem der Zeitpunkt der Unterschrift hervorgeht.

Aufgrund der o.a. Anforderungen an eine digitale Unterschrift muss es sich **mindestens um eine sogenannte fortgeschrittene elektronische Signatur** handeln, die eindeutig dem Unterzeichnenden zugeordnet werden kann und nachträgliche Änderungen erkennbar macht. Erläuterungen zu elektronischen Signaturen sind auch auf der Seite der Bundesdruckerei oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu finden:

www.bundesdruckerei.de/de/innovation-hub/die-verschiedenen-niveaus-der-digitalen-signatur#

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/ElektronischeSignatur/Glossar/esigglossar.html

Die Grundlage hierfür bildet die Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (die „eIDAS-Verordnung“ bzw. „IVT-Verordnung“).

Den Nachweis der **datenschutzkonformen Verwendung der Hard- und Software** muss der Maßnahmeträger erbringen. Die BA stellt keine eigenen Anforderungen an den Nachweis der Identität. Zudem handelt es sich jeweils um personenbezogene Daten, so dass der Maßnahmeträger ein Konzept für den datenschutzkonformen Einsatz haben sollte. Die Erstellung einer Datenschutzfolgenabschätzung wird empfohlen.[1]

Sachstand: November 2026

[1] Bei einer Datenschutzfolgenabschätzung handelt es sich um ein internes Dokument des Unternehmens zur Dokumentation der Risiken und des Umgangs mit der Datenverarbeitung. Die Einbindung externer Dienstleister oder Aufsichtsbehörden sind regelmäßig nicht erforderlich. Die Ausarbeitung obliegt dem Datenschutzbeauftragten des Unternehmens. Dabei handelt es sich lediglich um eine Empfehlung seitens der BA, kein zwingendes Erfordernis. Risiken für das Unternehmen im Falle einer Datenschutzverletzung können so ggf. minimiert werden.