MSP SSO

Die aktuelle Dokumentation des MSP SSO finden Sie hier als PDF-Dokument.pdf.

DSGVO-Maßnahmen

	Thema	Beschreibung/ Speicherung von Daten	Prozess	Lösung	Status
1	**SSO-Logfiles** Für Debugging und Entwicklung können Debugging-/Logging-Anweisungen im PHP-Code enthalten sein. Diese schreiben ihre Ausgaben in tagesaktuelle Logfiles.	**Löschen der Daten**	Die Logfiles werden automatisch nach 7 Tagen gelöscht.	Löschen der Logfiles per Cronjob jede Nacht.	✅
		Zugriff von außen	Das Logfile-Verzeichnis ist gegen Zugriff von außen gesichert.	Zugriffsschutz mittels htaccess-Datei im Logfile-Verzeichnis.	✅
2	**API-Logging** Die API bietet die Möglichkeit, zu Debugging-Zwecken alle Aufrufe mitzuloggen. Dies muss von einem Server-Administrator eingeschaltet werden. Dabei muss ein Filter gesetzt werden, der nur Daten mitloggt, auf den der Filter passt (z.B. eine E-Mail-Adresse).	**Löschen der Daten**	Die Logfiles werden automatisch nach 7 Tagen gelöscht.	Löschen der Logfiles per Cronjob jede Nacht.	✅
		Zugriff von außen	Das Logfile-Verzeichnis ist gegen Zugriff von außen gesichert.	Zugriffsschutz mittels htaccess-Datei im Logfile-Verzeichnis.	✅
3	**Webserver-Logfiles** Der Webserver loggt alle Requests mit den Standard-Einstellungen des Apache-Webservers mit. Ein Filter macht dabei evtl. übertragene Usernamen, E-Mail-Adressen und Passwörter unkenntlich. Einzig mitgeloggtes personenbezogenes Datum ist die IP-Adresse des Users.	**Löschen der Daten**	Die Logfiles werden automatisch nach 7 Tagen gelöscht.	Löschen der Logfiles per Cronjob jede Nacht.	✅
		Zugriff von außen	Das Logfile-Verzeichnis ist gegen Zugriff von außen gesichert.	Zugriffsschutz: Das Verzeichnis ist für den Webserver nicht erreichbar.	✅
4	**Export-Dateien/Dateien zum Download** Im SSO-Backend können Dateien exportiert werden:				
	• CSV-Export Benutzerkonten Hierüber kann eine CSV-Datei mit allen Benutzerkonten erstellt werden. Diese Datei enthält folgende personenbezogene Daten: UserID, GP-Nr, Loginname, Anrede, Titel, Vorname, Name, Strasse, Hausnummer, Postleitzahl, Ort, Land, Festnetz- und Mobilnummer, E-Mail, Datum der Konto-Aktivierung	**Löschen der Daten**	Mit dem Download wird die Datei automatisch vom Server gelöscht. Wird die Datei nicht heruntergeladen, wird sie nach 7 Tagen automatisch gelöscht.	Löschen der Export-Dateien nach dem Download oder per Cronjob jede Nacht.	✅
		Zugriff auf die Daten	Der Zugriff ist an ein Backend-Administrator-Login mit Rolle Super-Administrator geknüpft.	Administrator-Login mit Rolle Super-Administrator erforderlich.	✅

	• CSV-Export Daten eines einzelnen Benutzers	**Löschen der Daten**	Mit dem Download wird die Datei automatisch vom Server gelöscht. Wird die Datei nicht heruntergeladen, wird sie nach 7 Tagen automatisch gelöscht.	Löschen der Export-Dateien nach dem Download oder per Cronjob jede Nacht.	✅
		Zugriff auf die Daten	Der Zugriff ist an ein Backend-Administrator-Login geknüpft.	Administrator-Login erforderlich.	✅
5	**Registrierung** Pflichtfelder bei der Registrierung sind: Anrede, Vorname, Nachname, E-Mail-Adresse, selbst gewählter Benutzername, selbst gewähltes Passwort. Für die Registrierung muss die Datenschutzerklärung akzeptiert werden.	**Zugriff auf die Daten**	Die Daten werden einer Applikation nach Login über die API zur Verfügung gestellt. Die Applikation erhält dafür einen für die Login-Session des Users erstellten Zugriffsschlüssel. Die Applikation muss sich gegenüber der API mit einem eigenen Zugriffsschlüssel ausweisen. Pro Applikation ist weiterhin eingeschränkt, welche personenbezogenen Daten die Applikation sehen darf.	Login-Token eines Users und Applikations-Schlüssel einer Applikation für den Zugriff nötig.	✅
6	**Registrierung mit GP-Nummer** Bei der Registrierung kann der Kunde optional seine GP-Nummer angeben. Wird dies gemacht, prüft der SSO-Server die GP-Daten gegen das SAP-System. Kann die GP-Nummer verifiziert werden, werden Adress-Änderungen im SAP anschließend ins SSO synchronisiert.	**Zugriff auf die Daten**	Die Daten werden einer Applikation nach Login über die API zur Verfügung gestellt. Die Applikation erhält dafür einen für die Login-Session des Users erstellten Zugriffsschlüssel. Die Applikation muss sich gegenüber der API mit einem eigenen Zugriffsschlüssel ausweisen. Pro Applikation ist weiterhin eingeschränkt, welche personenbezogenen Daten die Applikation sehen darf.	Login-Token eines Users und Applikations-Schlüssel einer Applikation für den Zugriff nötig.	✅
		Löschen der Daten	Erfragt der User ein Löschen seiner Daten, werden alle Daten aus dem SSO gelöscht. Der benutzte Username und die E-Mail-Adresse werden dabei in einer anderen Tabelle gespeichert, die eine Neu-Registrierung mit diesen Benutzerdaten verhindert.	Blacklist mit gesperrten E-Mail-Adressen und Login-Namen.	✅
7	**Abgabe einer Werbe-EWE** Der Kunde kann bei der Registrierung eine Einwilligung erteilen, dass er mit einer Kontaktaufnahme seitens des Verlages bezüglich Werbung einverstanden ist.	**Zugriff auf die Daten**	Dem Kunden wird bei Einwilligung eine E-Mail zugesendet, in welcher er seine Entscheidung zur Einwilligung bestätigen muss. Dabei werden jeweils die Uhrzeit, IP-Adresse, versendete E-Mails und die Texte der akzeptierten EWE im SSO gespeichert.	Double-Opt-In.	✅
		Löschen der Daten	Die Einwilligung kann formlos durch z,B. eine E-Mail an den Verlag widerrufen werden.	E-Mail an widerruf@weser-kurier.de	✅
8	**User-Login** Beim Login wird ein sogenanntes Login-Token im JWT-Format erstellt, welches als Cookie im Browser des Users gespeichert wird. Dieses enthält personenbezogene Daten: Vorname, Nachname, Loginname, E-Mail-Adresse, UserId, Abo-Zugriffs-Rechte.	**Zugriff auf die Daten**	Die Daten werden einer Applikation nach Login über die API zur Verfügung gestellt. Die Applikation erhält dafür einen für die Login-Session des Users erstellten Zugriffsschlüssel. Die Applikation muss sich gegenüber der API mit einem eigenen Zugriffsschlüssel ausweisen. Pro Applikation ist weiterhin eingeschränkt, welche personenbezogenen Daten die Applikation sehen darf.	Login-Token eines Users und Applikations-Schlüssel einer Applikation für den Zugriff nötig.	✅
		Löschen der Daten	Das Login-Cookie wird nach dem Logout gelöscht oder nach Ablauf seiner Lebensdauer.	Cookie-Behandlung im Browser.	✅