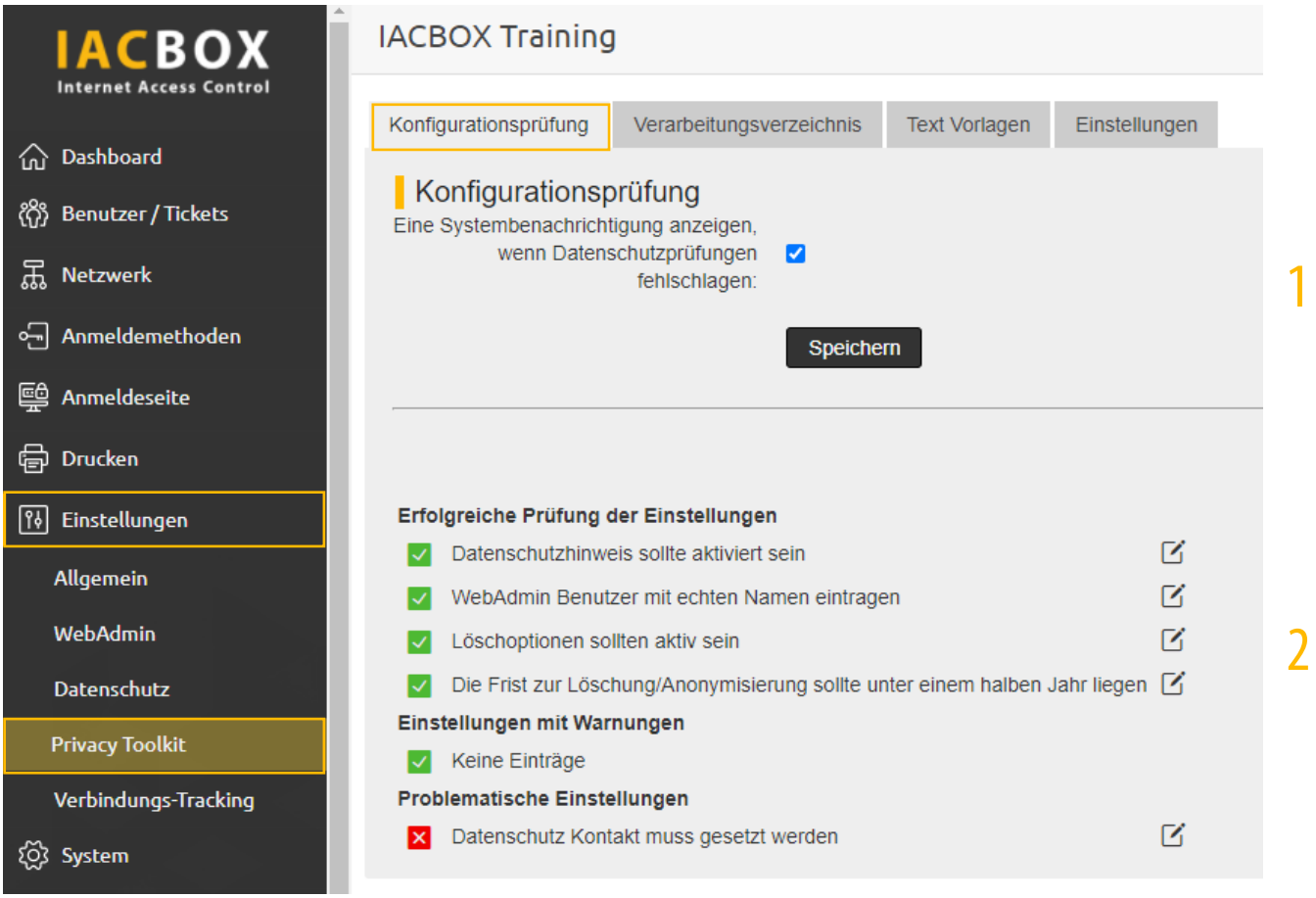
Privacy Toolkit

Schritt für Schritt zu Ihren passenden Einstellungen

Melden Sie sich im *WebAdmin* Ihrer IACBOX an. Unter dem Reiter Einstellungen finden Sie den Menüpunkt *Privacy Toolkit*. Sie benötigen dafür mindestens Version 17.2. Der Gesetzgeber schreibt neue Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen vor. Das Privacy Toolkit hilft Ihnen dabei, diese Regeln ordnungsgemäß einzuhalten.



Step 1 > Konfigurationsprüfung

Mit dieser Auswahl wird Ihnen im Bereich System Health eine Meldung angezeigt, sollten Sie eine kritische oder **falsche Einstellung vorgenommen haben.**

Step 2 > Konfigurationsprüfung > Erfolgreiche Prüfung der Einstellungen

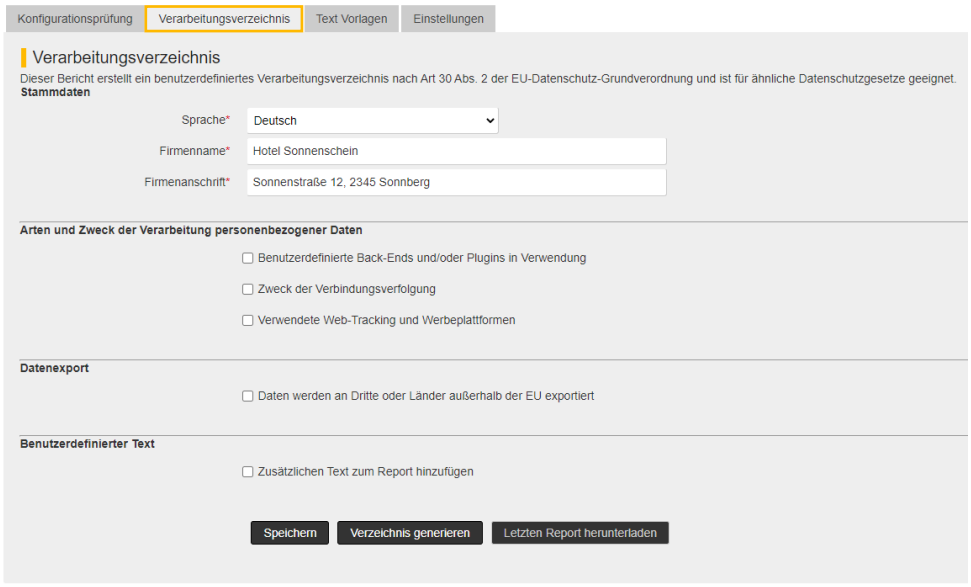
In diesem Bereich sehen Sie, ob die wichtigsten Einstellungen bezüglich Datenschutz richtig vorgenommen wurden. Bei Bedarf kommen Sie mit Klick auf das Edit Icon mit dem kleinen Bleistift rechts daneben in das jeweilige Menü und können Anpassungen vornehmen.

3

4

5

6



In diesem Menü kreieren Sie das Daten-verarbeitungs-verzeichnis.

Step 3 > Verarbeitungsverzeichnis > Stammdaten

Hier geben Sie die Firmendaten ein, welche auf dem Report angezeigt werden sollen. Im Sinne des Gesetzes ist der Betreiber des WLAN-Hotspots der Verantwortliche für die Datenverarbeitung.

Step 4 > Verarbeitungsverzeichnis > Arten und Zweck der Verarbeitung

Laut Artikel 30 DSGVO soll der Verantwortliche ein Datenverarbeitungsverzeichnis führen. Hier wird automatisch aufgelistet, welche Daten zu welchem Zweck vom System verarbeitet werden. Wenn Sie zusätzlich zu den Standard-Anmeldemethoden spezielle Backends verwenden (Login-API, CRM Datenbanken), können Sie diese hier eintragen und Zweck und Art der Verarbeitung beschreiben. Falls Sie die Verbindungsaufzeichnung aktiviert haben, können Sie hier Gründe angeben, warum bestimmte Daten gesammelt werden. Grundsätzlich ist es nicht verboten, Daten zu sammeln, es muss jedoch eine Rechtsgrundlage dafür geben (etwa Zustimmung des Nutzers) und es darf nicht ohne Wissen des Betroffenen erfolgen. Wenn auf Ihrer Anmeldeseite Web-Tracking und Werbeplattformen eingebunden sind, aktivieren Sie das entsprechende Textfeld und tragen Sie ebenfalls die Information dazu ein.

Step 5 > Privacy Reports > Datenexport

Geben Sie Daten an Drittfirmen weiter oder exportieren sie in Staaten außerhalb der EU, können Sie dies hier eintragen. Werden Daten an Dritte übertragen, muss der Betroffene informiert und einverstanden sein.

Step 6 > Privacy Reports > Benutzerdefinierte Text

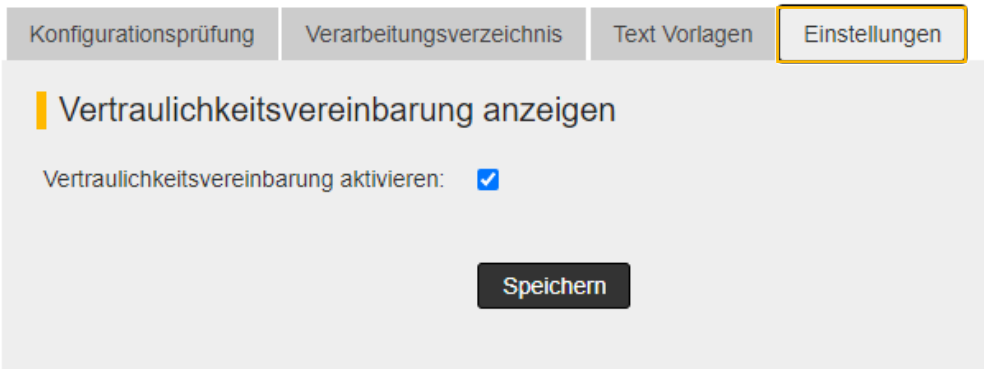
Nutzer müssen immer informiert sein, was mit ihren Daten passiert, daher können Verarbeitungsvorgänge, die nicht in eine der vorherigen Kategorien passt, hier eingetragen werden.

7

Step 7 > Text Vorlagen > Datenschutzbezogene Textvorlagen

Hier finden Sie den Volltext der DSGVO zum Nachschlagen, sowie andere nützliche Dokumente zum Herunterladen und Ausdrucken. Falls Sie Dritte mit der Verarbeitung von Nutzerdaten beauftragen, müssen Sie als Verantwortlicher sicherstellen, dass dies im Einklang mit der Verordnung erfolgt. Sie können dem Auftragsverarbeiter diese Mustervereinbarung vorlegen. Ebenso sind Sie gefordert, Angestellte oder Administratoren in Bezug auf die Vertraulichkeit der anvertrauten Daten zu unterweisen. Legen Sie diese Vertraulichkeitsvereinbarung jenen Mitarbeitern vor, die nicht die in Step 8 beschriebene Unterweisung sehen. Bei Verlust sensibler Daten oder sonstigen gravierenden Datenpannen sind Sie verpflichtet, die zuständige Datenschutzbehörde zu informieren. Dazu können Sie dieses Musterformular verwenden. Die zuständige nationale Behörde finden Sie ebenfalls in der hier abgelegten Liste.

8



Step 8 > Einstellungen > Vertraulichkeitsvereinbarung anzeigen

Meldet sich ein Admin zum ersten Mal im *WebAdmin* Interface an, muss er der Vertraulichkeitsvereinbarung zustimmen, um fortfahren zu können. Diese Abfrage ist standardmäßig aktiviert. Sie können Sie deaktivieren, falls Sie bereits anderweitig Vereinbarungen mit Mitarbeitern getroffen haben. Für alle Mitarbeiter, die Zugang zu Daten haben, aber keine Admins sind, verwenden Sie die Vereinbarung wie in *Step 7* beschrieben.

Hinweis > System Health

Ist eine Einstellung kritisch, erscheint im Bereich System Health ein Hinweis. Ist der Datenschutz betroffen, erkennen Sie das am farblich hinterlegten Wort PRIVACY. Mit Klick auf den Text gelangen Sie direkt in das entsprechende Menü.