imprivata®

Authentifizierung im Arbeitsalltag von Beschäftigten in operativen Positionen in Deutschland

Eine Studie von Imprivata und der FIDO Alliance zeigt, wie gemeinsam genutzte Zugänge, die Einführung passwortloser Authentifizierung und die Absicherung von Identitäten den Arbeitsalltag in Gesundheitseinrichtungen, der Fertigung und anderen systemrelevanten Branchen prägen.



VORWORT

Warum die Authentifizierung von Beschäftigten in operativen Positionen strategische Aufmerksamkeit verdient

Beschäftigte mit operativen Tätigkeiten halten Krankenhäuser, Fabriken, Logistiknetzwerke und andere systemrelevante Einrichtungen am Laufen. Sie arbeiten mit gemeinsam genutzten Arbeitsplatzrechnern und Mobilgeräten, klinischen Systemen und industrieller Betriebstechnik. Passt die Authentifizierung nicht zu diesen Abläufen, verlieren sie Zeit und umgehen Schutzmaßnahmen. Gleichzeitig wird für Unternehmen schwerer nachvollziehbar, wer auf ein System zugegriffen oder eine Aktion ausgeführt hat.

Imprivata und die FIDO Alliance haben untersucht, wie sich diese Herausforderungen in deutschen Unternehmen auswirken. Dafür befragten wir 150 Fach- und Führungskräfte auf mittlerer und oberer Ebene, die an Entscheidungen zu Authentifizierung, Identitätssicherheit oder Zugriffsmanagement beteiligt sind. Die Ergebnisse geben einen praxisnahen Einblick in die heutigen Arbeitsumgebungen und zeigen, welche Verbesserungen aus Sicht der Befragten den größten Nutzen hätten.

Drei Erkenntnisse stechen hervor. Erstens ist die gemeinsame Nutzung von Zugängen in Deutschland die Regel. In 91 Prozent der Unternehmen wird mindestens ein Endpunkt gemeinsam genutzt. Fast die Hälfte gibt an, dass die meisten oder nahezu alle Beschäftigten im operativen Bereich solche Geräte verwenden. Zweitens gewinnt passwortlose Authentifizierung an Bedeutung. Meist ist sie jedoch Teil einer gemischten Umgebung und ersetzt Passwörter noch nicht vollständig. Drittens ist eine umständliche Authentifizierung zugleich ein Betriebs- und Sicherheitsthema. Deutsche Unternehmen schätzen, dass durchschnittlich fast 38 Prozent ihrer Frontline-Mitarbeitenden in einem typischen Monat mindestens ein authentifizierungsbezogenes Problem erleben.

Je nach Branche stellen sich diese Entwicklungen unterschiedlich dar. Im Gesundheitswesen muss das Identitäts- und Zugriffsmanagement schnelle klinische Abläufe unterstützen. Gemeinsam genutzte Arbeitsplätze und Schutzausrüstung prägen dabei die Anforderungen. In der Fertigung ist die Belastung am größten: Monatlich sind 45 Prozent der Beschäftigten auf der operativen Ebene betroffen. Vorhandene Geräte und Anwendungen unterstützen geeignete Authentifizierungsverfahren häufig nicht. In anderen Branchen ist die gemeinsame Nutzung weniger verbreitet. Dafür stehen schnelle Abläufe, sichere Sitzungen und der Schutz vor KI-gestütztem Identitätsmissbrauch stärker im Fokus. Zusammengenommen ordnen die Ergebnisse wichtige Zugriffsfragen in Deutschland ein: vom Zugang ab dem ersten Arbeitstag über NIS2- und KRITIS-Maßnahmen bis hin zur Transformation des Gesundheitswesens sowie zum sicheren mobilen und gemeinsam genutzten Zugriff.

Unternehmen sollten die Ergebnisse als Ausgangspunkt für konkrete Verbesserungen nutzen. Es geht nicht darum, überall dieselbe Authentifizierungsmethode einzusetzen. Ziel ist ein Zugang, der schnell genug für die Arbeit in direktem Kontakt mit Patienten oder Kunden, an der Fertigungsstraße oder am Fließband ist, auf modernen wie älteren Systemen funktioniert und zugleich die persönliche Verantwortlichkeit sicherstellt. Dafür müssen Unternehmen den Benutzerwechsel und die Übergabe gemeinsam genutzter Geräte ebenso berücksichtigen wie die Kontowiederherstellung, die Identitätsprüfung durch den Service Desk und die lückenlose Protokollierung jedes Zugriffs.

Für IT- und Sicherheitsverantwortliche in Deutschland besteht die Chance darin, betriebliche und sicherheitsbezogene Ziele gleichzeitig zu verfolgen. Maßnahmen, die Zeitverluste verringern, können auch das Teilen von Zugangsdaten, unbeaufsichtigte Sitzungen und Unklarheit über Zugriffe auf sensible Systeme reduzieren. Eine mehrheitlich einheitliche Authentifizierung sorgt für mehr Sicherheit der IT-Systeme im Arbeitsalltag. Vor allem für regulierte Unternehmen, die die Anforderungen von NIS2 und KRITIS umsetzen, wird ein konsistenter Zugang zu einem wichtigen Baustein.

Wir hoffen, dass dieser Bericht Ihnen hilft, Ihre Umgebung mit der anderer Unternehmen zu vergleichen, risikobehaftete Reibungspunkte zu erkennen und die nächsten Schritte Ihrer Strategie für Identitätssicherheit gezielter zu planen.

Mit freundlichen Grüßen



Joel Burleson-Davis

Chief Technology & Security Officer
Imprivata

EINLEITUNG

Deutsche Unternehmen sehen sich regelmäßig mit einem hohen Aufwand rund um die Authentifizierung konfrontiert. Gemeinsam genutzte Endpunkte sind hier verbreiteter als in der globalen Stichprobe. Die Umstellung auf passwortlose Verfahren schreitet voran, ist aber noch nicht abgeschlossen. Am deutlichsten ist der Wunsch nach einem einheitlichen Zugang über Geräte und Anwendungen hinweg.

91%

Unternehmen mit mindestens einem gemeinsam genutzten Endpunkt

65%

Unternehmen mit passwortbasierter oder uneinheitlicher Authentifizierung beziehungsweise ohne konsequente Authentifizierungspflicht

37,9%

Durchschnittlicher Anteil monatlich von Authentifizierungsproblemen betroffener Beschäftigter in operativen Tätigkeiten

In deutschen Unternehmen des Gesundheitswesens und der Fertigung sind gemeinsam genutzte Zugänge nahezu überall verbreitet. Die betrieblichen Herausforderungen unterscheiden sich jedoch: Im Gesundheitswesen ergeben sich besondere Anforderungen aus dem klinischen Alltag. In der Fertigung muss die Authentifizierung in einer heterogenen Umgebung aus Arbeitsplatzrechnern, Mobilgeräten und industrieller Betriebstechnik funktionieren. Das erklärt auch, warum der Zugang für übergeordnete Vorhaben in Deutschland strategisch an Bedeutung gewinnt. Ein reibungsloser Start am ersten Arbeitstag und Rollenwechsel setzen eine durchgängige Identität über HR- oder IGA-Prozesse, KIS und Fachanwendungen hinweg voraus. NIS2 und KRITIS rücken Zugriffskontrolle, Nachweisbarkeit, Resilienz und Verantwortlichkeit in den betrieblichen Fokus. Zusammenschlüsse im Zuge von KHVVG und KHAG können standortübergreifende Zugriffe, Shared Services und mobile Zugänge zusätzlich komplexer machen.



Gesundheitswesen



92% nutzen gemeinsam verwendete Endpunkte

33% haben Schwierigkeiten bei der Authentifizierung mit Handschuhen oder Schutzausrüstung

Fertigung



97% nutzen gemeinsam verwendete Geräte. Bei nur 34 % sind diese für die meisten Beschäftigten in der operativen Praxis vorgesehen.

26% der operativ Beschäftigten erlebten Verzögerungen beim Wechsel zwischen gemeinsam genutzten und persönlichen Geräten

Die wichtigsten Erkenntnisse für IT- und Sicherheitsverantwortliche:

- Gemeinsam genutzte Endpunkte sind weit verbreitet, individuelle Authentifizierung ist jedoch noch nicht selbstverständlich.
- Unternehmen stellen schrittweise auf passwortlose Authentifizierung um, nutzen Passwörter aber weiterhin.
- Der deutlichste genannte Vorteil passwortloser Authentifizierung ist eine höhere Produktivität.
- Umständliche Authentifizierung betrifft viele Beschäftigte und summiert sich mit der Zeit.
- Ausweichlösungen machen aus Bedienproblemen ein Risiko für die Identitätssicherheit.
- In Deutschland ist die Sorge vor Identitätsmissbrauch geringer als in der globalen Stichprobe. Dennoch berichtet eine Mehrheit von vermuteten oder bestätigten Vorfällen bei Wiederherstellung, Zurücksetzung oder Identitätsvortäuschung.

Gemeinsam genutzte Endpunkte sind üblich, persönliche Verantwortlichkeit bleibt jedoch schwer sicherzustellen

Gemeinsam genutzte Endpunkte sind für Beschäftigte mit einem operativen Schwerpunkt in Deutschland weit verbreitet. Die Nutzung unterscheidet sich jedoch je nach Branche. Mehr als die Hälfte der Unternehmen im Gesundheitswesen (54 %) gibt an, dass nahezu all diese Beschäftigten gemeinsam genutzte Geräte verwenden. In der Fertigung sind solche Geräte zwar fast überall im Einsatz (97 %), doch die Geräteumgebung ist stärker gemischt. Nur 34 % der Unternehmen sagen, dass nahezu alle Mitarbeitende in der Produktion Geräte gemeinsam nutzen.



In Deutschland greift das operative Personal auf zahlreiche betriebliche Systeme zu. Am häufigsten sind Sicherheits-, Compliance- und Berichtssysteme (61 %). Es folgen Kommunikations- und Kollaborationstools (52 %) sowie Zeiterfassungs- oder Personalmanagementsysteme (52 %). Klinische Anwendungen und elektronische Patientenakten kommen auf 35 %, Systeme der industriellen Betriebstechnik auf 30 %.

Gemeinsam genutzte Zugänge spielen eine besonders große Rolle. In 91 % der deutschen Unternehmen wird mindestens ein Endpunkt gemeinsam genutzt. Dazu zählen Computer oder Arbeitsplätze (63 %) sowie mobile Geräte, Scanner oder Handhelds (57 %). Von den Unternehmen mit gemeinsam genutzten Endpunkten geben 48 % an, dass die meisten oder nahezu alle operativ Beschäftigten diese Geräte verwenden.

Dieses Betriebsmodell erschwert die Zuordnung von Aktivitäten auf konkrete Personen. Nur 33 % der deutschen Unternehmen geben an, dass alle oder nahezu alle operativ Beschäftigten ein eigenes Konto beziehungsweise eigene Zugangsdaten verwenden. Am häufigsten verhindern allgemeine Produktivitäts- oder Workflow-Hürden (44 %) eine konsequente Nutzung individueller Zugangsdaten. Es folgen fehlende Unterstützung geeigneter Authentifizierungsmethoden auf vorhandenen Geräten oder in Anwendungen (36 %) und die schwierige Authentifizierung an Geräten, die viele Personen gemeinsam nutzen (35 %).

	Gesundheitswesen	Fertigung	Andere Branchen
Aktive gemeinsame Endpunkte	92%	97%	81%
Gemeinsam genutzte Endpunkte für die meisten oder nahezu alle Beschäftigten	54%	34%	–
Alle oder nahezu alle Beschäftigten nutzen individuelle Zugangsdaten	36%	21%	42%

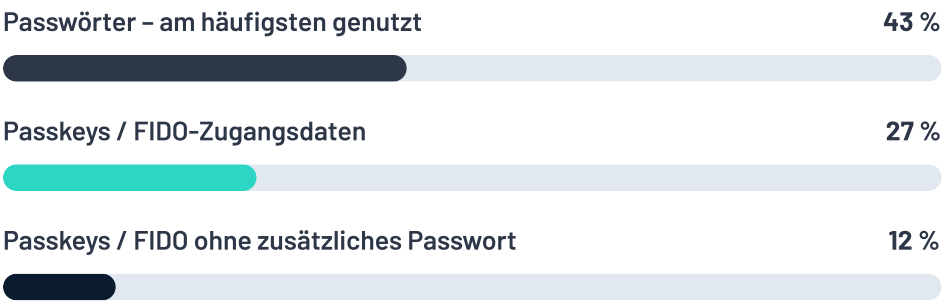
Einführung und Nutzen passwortloser Verfahren

Deutsche Unternehmen führen zunehmend passwortlose Authentifizierungsverfahren ein. Die Hürden sind dabei je nach Branche unterschiedlich. Im Gesundheitswesen erschweren ältere Systeme und bestehende Abläufe die Umstellung. In der Fertigung sind Kompatibilitätsprobleme mit Geräten besonders ausgeprägt. Risiken rund um Kontowiederherstellung und Sitzungen betreffen alle Branchen.

Bei 65 % der deutschen Unternehmen basiert die Authentifizierung weiterhin auf Passwörtern, sie erfolgt uneinheitlich oder wird nicht konsequent verlangt. 18 % bezeichnen ihren Ansatz als überwiegend oder vollständig passwortlos. Weltweit sind es 14 %. Der Wandel ist also im Gange. Die meisten Unternehmen müssen den Übergang jedoch weiterhin für gemeinsam genutzte Geräte, ältere Anwendungen und unterschiedliche operative Arbeitsabläufe in die Praxis umsetzen.

Passwort-Methoden im Vergleich

Deutsche Unternehmen



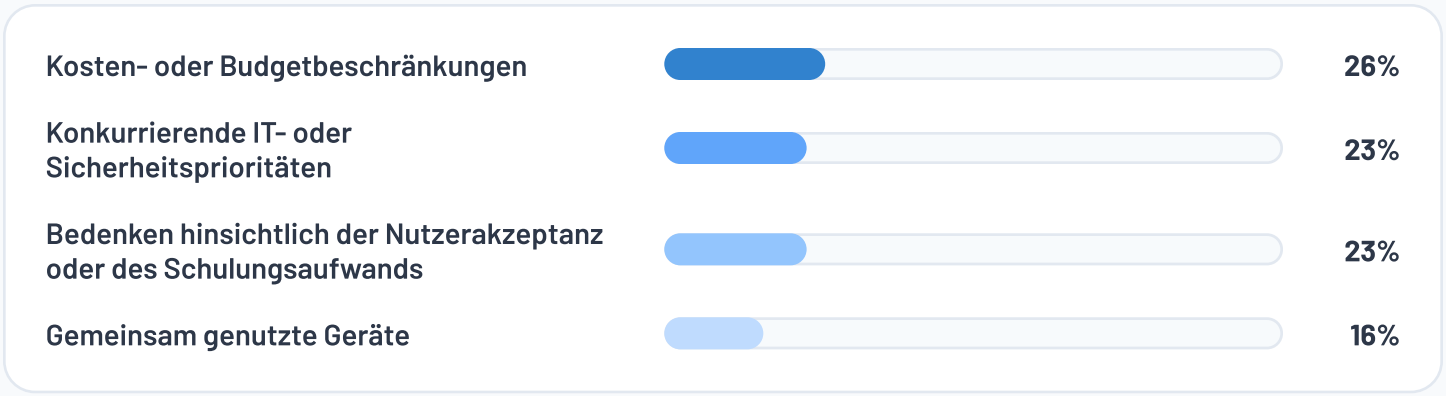
Eine moderne Methode allein bedeutet also noch nicht, dass die Abhängigkeit von Passwörtern entfällt.



Passwörter sind mit Eine moderne Methode allein bedeutet also noch nicht, dass die Abhängigkeit von Passwörtern entfällt.

Nutzen im Betriebsalltag

Höhere Produktivität der Beschäftigten im operativen Bereich	39 %
Schnellerer Zugriff	32 %
Bessere Compliance oder Auditierbarkeit	29 %
Bessere Nachvollziehbarkeit individueller Zugriffe	28 %



Branche	Größter erwarteter Nutzen	Größte Einführungshürde
Gesundheitswesen	**39 %** Schnellerer Zugriff	Ältere Systeme, Geräte oder Anwendungen **29 %**
Fertigung	**44 %** Compliance oder Auditierbarkeit	Vorhandene Geräte oder Anwendungen unterstützen geeignete Verfahren nicht **55 %**
Andere Branchen	**44 %** Produktivität	Unsicherheit bei Compliance oder Regulierung **36 %**

Authentifizierungsprobleme betreffen viele Beschäftigte und stören Arbeitsabläufe immer wieder

Die Belastung durch Authentifizierung ist weit verbreitet und kein Einzelfall. Im Durchschnitt sind in einem typischen Monat knapp vier von zehn Beschäftigten im operativen Bereich betroffen. 39 % der Unternehmen geben an, dass mindestens die Hälfte ihres operativen Personals betroffen ist.



Insgesamt schätzen deutsche Unternehmen, dass 38 % ihrer operativ Beschäftigten in einem typischen Monat mindestens ein authentifizierungsbezogenes Problem erleben. In der Fertigung ist der Anteil betroffener Beschäftigter und die Häufigkeit von Unterbrechungen am höchsten.

Am häufigsten sind Verzögerungen beim Wechsel zwischen Geräten oder Arbeitsplätzen (29 %), Verbindungsprobleme mit fehlgeschlagener Authentifizierung (27 %) sowie Verzögerungen beim Benutzerwechsel an gemeinsam genutzten Geräten und Schwierigkeiten bei der Authentifizierung mit Handschuhen oder Schutzausrüstung (je 25 %). Diese Probleme treten mitten im Arbeitsablauf auf und nicht nur bei der ersten Anmeldung.

Unter den betroffenen Beschäftigten erleben 63 % mindestens wöchentlich Unterbrechungen. Im Durchschnitt werden 9,5 Unterbrechungen pro Monat gemeldet, bei einem Zeitverlust von 13,3 Minuten je Vorfall. Zusammengenommen entspricht das beispielhaft einer Belastung von rund 127 Minuten oder 2,1 Stunden pro betroffene Person und Monat.

2,1

Stunden pro betroffene Person und Monat.

höhere Auslastung der IT oder des Service Desks
32 %

Verzögerungen in der Patientenversorgung, Produktion, Lieferung oder anderen Tätigkeiten
30 %

eingeschränkte Nachverfolgung von Benutzeraktivitäten
29 %

geringere Mitarbeiterzufriedenheit
29 %

Betriebliche Kennzahl	Gesundheitswesen	Fertigung
Monatlich von Authentifizierungsproblemen betroffene Beschäftigte	35 %	45 %
Unterbrechungen je betroffener Person und Monat	9,4	12,5
Zeitverlust je Vorfall in Minuten	13,2	14,5
Größte betriebliche Auswirkung	Höhere Auslastung der IT/des Service Desks (34%)	Höheres Sicherheitsrisiko (37%)

Ausweichlösungen und Wiederherstellungsprozesse zeigen die Grenzen einer Sicherheit, die sich auf die Anmeldung beschränkt

IT- und Sicherheitsverantwortliche sind insgesamt zuversichtlich, Zugriffe einzelnen Personen zuordnen zu können. Die zugrunde liegenden Risiken unterscheiden sich jedoch je nach Branche. Im Gesundheitswesen stehen gemeinsam genutzte Zugangsdaten und mangelnde Transparenz im Vordergrund. In der Fertigung geht es vor allem um Zugriffe auf gemeinsam genutzte Geräte und Compliance. Andere Branchen sorgen sich stärker um Kontoübernahmen, unbeaufsichtigte Sitzungen und KI-gestützte Identitätsvortäuschung.

Umständliche Authentifizierung beeinflusst das Verhalten. Deutsche Unternehmen beobachten, dass Beschäftigte die Mehr-Faktor-Authentifizierung oder andere Schutzmaßnahmen umgehen (**33 %**), Zugangsdaten teilen oder Passwörter wiederverwenden (je **31 %**), angemeldet bleiben, um eine erneute Authentifizierung zu vermeiden (**30 %**), oder die Systemnutzung vermeiden beziehungsweise aufschieben (**30 %**). Nur **6 %** beobachten keines dieser Verhaltensmuster. Die größte Sorge im Bereich Identitätssicherheit gilt gemeinsam genutzten Zugangsdaten oder Konten (**33 %**). Es folgen unbefugte Zugriffe auf gemeinsam genutzte Geräte (**29 %**) und mangelnde Transparenz darüber, wer auf ein System zugegriffen hat (**27 %**).

Auch die Kontowiederherstellung ist ein kritischer Punkt. Mehr als die Hälfte der Unternehmen berichtet von einem bestätigten oder vermuteten Vorfall im Zusammenhang mit dem Service Desk, der Kontowiederherstellung, dem Zurücksetzen der Mehr-Faktor-Authentifizierung und/oder KI-gestützter Identitätsvortäuschung innerhalb der vergangenen zwölf Monate.

Geplante Investitionen in Identitätssicherheit

Anteil der Organisationen, die in folgende Bereiche investieren wollen



Weltweit: 28% (Passkeys/FIDO)

Sicheren Zugang im Arbeitsalltag praktikabel gestalten

Die Studienergebnisse weisen deutschen Unternehmen eine klare Richtung. Die Authentifizierung von Beschäftigten im operativen Bereich muss auf gemeinsam genutzten und persönlichen Endgeräten, in modernen und älteren Systemen sowie in zeitkritischen Abläufen funktionieren. Eine Strategie, die nur den Passwortersatz in den Blick nimmt, greift zu kurz. Die Ergebnisse stehen zudem im Zusammenhang mit vier wichtigen Themen in Deutschland: Zugang ab dem ersten Arbeitstag, Vorbereitung auf NIS2 und KRITIS, die Transformation des Gesundheitswesens im Zuge von KHVVG und KHAG sowie Enterprise Access Management und mobiler klinischer Zugriff.

An erster Stelle steht ein einheitlicher Zugang. Deutsche Unternehmen wünschen sich vor allem eine konsistente Authentifizierung über Geräte und Anwendungen hinweg. Dazu gehört, unnötige Unterschiede beim Anmelden, beim Benutzerwechsel, bei der Kontowiederherstellung und beim Wechsel zwischen Systemen abzubauen.

Zweitens muss jeder Zugriff einer Person zugeordnet werden können. Gemeinsam genutzte Endpunkte sind weit verbreitet. Zu den größten Bedenken zählen gemeinsam genutzte Zugangsdaten, unbefugte Zugriffe auf gemeinsam genutzte Geräte und die eingeschränkte Transparenz darüber, wer auf Systeme zugreift. Benutzerwechsel müssen schnell gehen. Dabei muss jedoch die vorherige Sitzung beendet und die Identität der nächsten Person festgestellt werden.

Drittens muss die Sicherheit über die erste Anmeldung hinaus gewährleistet sein. Wiederherstellung, Zurücksetzung, Registrierung für die Mehr-Faktor-Authentifizierung und Kontakte mit dem Service Desk sind ebenfalls Zugriffsereignisse. Bei uneinheitlicher Identitätsprüfung können sie die Sicherheit schwächen. Deutsche Unternehmen berichten von unterschiedlichen Wiederherstellungsverfahren und zahlreichen vermuteten oder bestätigten Vorfällen über diese Kanäle.





Viertens ergänzen sich betrieblicher Nutzen und Sicherheitsgewinn. Die Befragten verbinden passwortlose Authentifizierung vor allem mit höherer Produktivität der Beschäftigten. Eine reibungsarme Anmeldung spart Zeit und kann zugleich das Teilen von Zugangsdaten, das Umgehen von Schutzmaßnahmen, unbeaufsichtigte Sitzungen und Unklarheit darüber verringern, wer eine Aktion ausgeführt hat.

Fragen für die Diskussion auf Führungsebene

- Bei welchen Übergaben gemeinsam genutzter Geräte entstehen die größten Verzögerungen oder Lücken bei der Zuordnung?
- In welchen operativen Arbeitsabläufen ist weiterhin ein Passwort erforderlich, obwohl ein stärkeres Verfahren verfügbar ist?
- Wie einheitlich wird die Identität beim Zurücksetzen von Passwörtern, beim Entsperren von Konten und bei der Registrierung für die Mehr-Faktor-Authentifizierung geprüft?
- Kann das Unternehmen nachweisen, wer von welchem Gerät aus und während welcher Sitzung auf ein System zugegriffen hat?
- Welche Verbesserung würde einen sicheren Zugriff für operativ Beschäftigte zur praktikablen Lösung machen?

imprivata®

Imprivata, das Unternehmen für digitale Identität im Gesundheitswesen, bietet Lösungen für Identitäts-, Authentifizierungs- und Zugriffsmanagement, die speziell für die besonderen Herausforderungen des Gesundheitswesens in den Bereichen Workflow, Sicherheit und Compliance entwickelt wurden.

Für weitere Informationen kontaktieren Sie uns bitte unter:

Global headquarters USA
Waltham, MA
Phone: +1 877 663 7446
www.imprivata.com

European headquarters
Uxbridge, England
Phone: +44 (0)208 744 6500
www.imprivata.com/uk

Germany
Langenfeld
Phone: +49 (0) 2173 99 385 0
www.imprivata.com/de

Australia
Melbourne
Phone: +613 8844 5533

Copyright © 2026 Imprivata, Inc. Alle Rechte vorbehalten. Imprivata ist eingetragene Marke von Imprivata, Inc. in den USA und anderen Ländern. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.