GROSSENBACHER
RECHTSANWÄLTE

NEWSLETTER NOVEMBER 2026



DIGITALE PRODUKTE - NEUE PFLICHTEN FÜR SICHERHEIT UND DATEN IN DER EU

TRANSPARENZREGISTER UND NEUE GWG-PFLICHTEN

VERSTÄRKUNG UNSERES TEAMS

IT & Datenschutz

DIGITALE PRODUKTE - NEUE PFLICHTEN FÜR SICHERHEIT UND DATEN IN DER EU

Thomas Merz · Rechtsanwalt · Notar

Von der Kaffeemaschine bis zur Industrieanlage sind immer mehr Produkte intelligent und mit dem Internet verbunden. Die EU sah darin Handlungsbedarf und verabschiedete mehrere Verordnungen. Der Cyber Resilience Act (CRA) verlangt, dass solche Produkte gegen Cyberangriffe besser geschützt werden. Der Data Act legt hingegen fest, wer die Daten nutzen darf, die beim Gebrauch solcher Produkte entstehen. Werden Produkte zudem mit künstlicher Intelligenz ausgestattet, ist auch der AI Act zu beachten. Alle drei Verordnungen stellen Unternehmen vor neue Herausforderungen. Dieser Beitrag gibt einen Überblick über die wichtigsten Pflichten und Fristen, die unter bestimmten Voraussetzungen auch für Schweizer Unternehmen gelten.



CYBER RESILIENCE ACT (CRA)

Viele Produkte kommen mit bekannten Sicherheitslücken auf den Markt und Updates bleiben oft schon nach kurzer Zeit aus. Gehackte Babyphones, lahmgelegte Streamingdienste oder offengelegte Kundendaten sind die Folge. Die EU legt mit dem CRA erstmals Mindestanforderungen an die Cybersicherheit fest. Die Sicherheit wird damit zur Voraussetzung für den Marktzugang. Erfasst ist fast alles, was sich mit dem Internet oder einem anderen Gerät verbinden lässt. Das Gesetz spricht von Produkten mit digitalen Elementen. Dazu gehören vernetzte Geräte wie ein Smart-TV, reine Software wie Apps sowie die Cloud-Dienste, die der Hersteller für sein Produkt betreibt. Ausgenommen sind vor allem Produkte mit eigenen Sicherheitsregeln, etwa Medizinprodukte und Kraftfahrzeuge.

Die Verantwortung für die Cybersicherheit liegt beim Hersteller. Bereits bei der Entwicklung muss er die Risiken prüfen und für die Sicherheit seines Produkts sorgen. Beim Verkauf dürfen keine bekannten ausnutzbaren Schwachstellen bestehen. Produkte müssen mit sicheren Voreinstellungen ausgeliefert und vor unbefugtem Zugriff geschützt werden. Auch nach dem Verkauf bleibt der Hersteller in der Pflicht. Während einer festgelegten Zeit muss er Sicherheitslücken beheben und kostenlose Updates liefern. Diese Zeit richtet sich nach der erwarteten Nutzungsdauer und beträgt in der Regel mindestens fünf Jahre. Werden Schwachstellen aktiv ausgenutzt oder kommt es zu einem schweren Sicherheitsvorfall, muss der Hersteller dies über die zentrale Plattform der Cybersicherheitsagentur der EU (ENISA) melden. Betroffene Personen sind ebenfalls zu informieren.

Ob ein Produkt die Anforderungen erfüllt, zeigt künftig die CE-Kennzeichnung. In den meisten Fällen bringt der Hersteller sie in eigener Verantwortung an. Er bestätigt damit selbst, dass alle Vorgaben eingehalten sind. Nur bei besonders sicherheitsrelevanten Produkten wie Firewalls oder Passwortmanagern kann eine Prüfung durch eine unabhängige Prüfstelle nötig sein.

Der CRA kann auch Schweizer Unternehmen tangieren. Entscheidend ist nicht der Sitz eines Unternehmens, sondern ob Produkte in der EU verkauft oder vertrieben werden. Schweizer Zulieferer können auch indirekt betroffen sein, wenn ihre Abnehmer in der EU entsprechende Nachweise verlangen. Für bestehende Produkte gelten die neuen Anforderungen grundsätzlich erst, wenn wesentliche Änderungen vorgenommen werden. Massgebend dabei ist, ob eine Änderung das Sicherheitsrisiko erhöht. Das kann bereits bei einem Update mit neuer Cloud-Anbindung oder zusätzlicher Schnittstelle der Fall sein. Reine Sicherheitsupdates und Reparaturen gelten in der Regel nicht als wesentliche Änderung. Anders ist es bei der Pflicht, ausgenutzte Sicherheitslücken zu melden. Sie gilt auch für Produkte, die bereits auf dem Markt sind.

DATA ACT

Vernetzte Produkte sind Geräte, die Daten über ihre Nutzung erfassen und weitergeben können, zum Beispiel ein Auto, das Fahrdaten speichert, oder eine Wärmepumpe, die ihren Verbrauch aufzeichnet. Erfasst sind auch sogenannte verbundene Dienste. Das sind digitale Dienste, die zu einem vernetzten Produkt gehören, etwa eine Smart-Home-App. Bisher verfügte über diese Daten meist allein der Hersteller.

Neu erhalten Privatpersonen und Unternehmen, die ein solches Produkt nutzen, kostenlosen Zugang zu diesen Daten. Sie können zudem verlangen, dass die Daten an Dritte weitergegeben werden, etwa an eine unabhängige Werkstatt oder einen anderen Serviceanbieter. Neue

Produkte müssen deshalb so gestaltet sein, dass dieser Zugang einfach und sicher möglich ist. Schon vor dem Kauf muss erkennbar sein, welche Daten erzeugt werden und wie darauf zugegriffen werden kann. Der Data Act setzt dem Hersteller damit Grenzen, schützt aber auch seine Interessen. Zum einen darf er die Daten nicht mehr nach Belieben selbst nutzen. Dafür braucht er eine Vereinbarung mit der Kundschaft. Zum anderen bleiben seine Geschäftsgeheimnisse geschützt. Betriebsdaten können etwa verraten, wie eine Maschine im Detail funktioniert. Solche Daten muss der Hersteller nur herausgeben, wenn mit dem Empfänger geeignete Schutzmassnahmen vereinbart sind, etwa eine Vertraulichkeitsvereinbarung. Nur in Ausnahmefällen ist die Verweigerung der Herausgabe zulässig. Für die Weitergabe an Dritte kann zudem eine Vergütung verlangt werden.

Wer vernetzte Produkte oder verbundene Dienste in der EU anbietet, ist betroffen – und zwar ebenfalls unabhängig vom Sitz des Unternehmens. Schweizer Zulieferer und Dienstleister können den Data Act auch indirekt spüren, wenn ihre EU-Partner die Pflichten vertraglich weitergeben. Umgekehrt können Schweizer Serviceanbieter keinen Zugang zu Daten verlangen, da dieses Recht nur für Empfänger innerhalb der EU gilt. Schweizer Unternehmen sollten den Datenzugang deshalb mit ihren EU-Partnern vertraglich sichern. Besonders spürbar wird der Data Act bei Reparatur und Wartung. Viele Geräte lassen sich heute nur noch reparieren, wenn ihre Daten mit einem Diagnosegerät ausgelesen werden. Bisher kontrollierten oft allein die Hersteller diesen Zugang und damit auch, wer Reparaturen anbieten konnte. In der Automobilindustrie erhielten freie Werkstätten deshalb schon vor Jahren Zugang zu den nötigen Informationen. Der Data Act überträgt diesen Gedanken auf weitere Produkte. Neu können beispielsweise Landwirtschaftsbetriebe für Landmaschinen verlangen, dass auch unabhängige Werkstätten Zugang zu den Daten erhalten. Fällt ein Traktor mitten in der Ernte aus, müssen sie nicht mehr auf den Hersteller warten. Für Hersteller bedeutet das mehr Konkurrenz im Servicegeschäft, für Privatpersonen mehr Wahlfreiheit und im besten Fall günstigere Angebote.

AI ACT

Der AI Act regelt den Einsatz künstlicher Intelligenz. Er folgt einem einfachen Grundsatz. Je grösser das Risiko für Menschen, desto strenger die Regeln. Für die meisten KI-Anwendungen, etwa Spamfilter oder Videospiele, gelten deshalb keine besonderen Pflichten. Einige Anwendungen sind dagegen ganz verboten. Dazu gehört etwa die Bewertung von Menschen nach ihrem sozialen Verhalten. Dazwischen liegen die sogenannten Hochrisiko-KI-Systeme. Sie entscheiden über wichtige Fragen im Leben von Menschen mit oder betreffen deren Sicherheit, etwa bei der Auswahl von Bewerbenden oder als Sicherheitsbauteil einer Maschine. Für sie gelten strenge Anforderungen.

Für Privatpersonen sind vor allem die Transparenzpflichten spürbar. Wer mit einem Chatbot schreibt, muss erkennen können, dass am anderen Ende eine Maschine antwortet. Täuschend echte Bilder oder Videos, die mit KI erzeugt wurden, müssen als solche gekennzeichnet sein. Wie beim CRA und beim Data Act ist auch hier nicht der Sitz entscheidend. Schweizer Unternehmen sind betroffen, wenn sie KI-Systeme in der EU anbieten. Dasselbe gilt, wenn die Ergebnisse ihrer KI-Systeme in der EU verwendet werden.

PRIVATPERSONEN IN DER SCHWEIZ

Als EU-Verordnungen schützen CRA, Data Act und AI Act Privatpersonen in der Schweiz nicht direkt.





So gewährt ihnen der Data Act grundsätzlich kein Recht auf Zugang zu den Daten ihrer vernetzten Geräte, auch wenn sie diese in der EU gekauft haben. Immerhin können ihnen die Sicherheitsanforderungen des CRA und die Transparenzpflichten des AI Acts aber indirekt zugutekommen, wenn Hersteller und Anbieter in der Schweiz dieselben Produkte und Dienste vertreiben wie in der EU.

FAZIT

Der CRA sorgt für mehr Sicherheit. Der Data Act schafft Zugang zu Nutzungsdaten. Der AI Act setzt Regeln für den Einsatz künstlicher Intelligenz. Für Unternehmen bringt es neue Pflichten, deren Umsetzung bereits begonnen hat und schrittweise erfolgt. Unter anderem gehören folgende wichtige Daten in jede Agenda:

• Beim CRA gelten die Meldepflichten seit dem 11. September 2026. Alle übrigen Herstellerpflichten gelten ab dem 11. Dezember 2027.
• Der Data Act gilt seit dem 12. September 2025. Neu in Verkehr gebrachte Produkte müssen den direkten Datenzugriff seit dem 12. September 2026 ermöglichen.
• Beim AI Act gelten die Verbote bereits seit Februar 2025 und die Transparenzpflichten seit August 2026. Die Pflichten für Hochrisiko-KI-Systeme gelten ab Dezember 2027 und für KI in Produkten, beispielsweise in Spielzeugen, ab August 2028.

Die Verordnungen sind also bereits in Kraft getreten und teilweise bereits anwendbar, lassen aber viele Fragen offen. Die Europäische Kommission will Leitlinien herausgeben, um diese zu beantworten. Das gelingt unterschiedlich gut:

• Beim CRA gibt es einen Fragenkatalog (FAQ). Im Juli 2026 publizierte die Europäische Kommission zudem englische Leitlinien, die formell noch nicht verabschiedet sind. Die technischen Normen fehlen ebenfalls noch. Sie sollen EU-weit festlegen, wie die Sicherheitsanforderungen erfüllt werden können. Hält ein Hersteller diese Normen ein, wird davon ausgegangen, dass sein Produkt die entsprechenden Anforderungen des CRA erfüllt. Bis dahin muss der Hersteller selbst begründen, warum sein Produkt den Anforderungen entspricht, gegebenenfalls durch Drittprüfungen.
• Beim Data Act gibt es ebenfalls einen Fragenkatalog und Vorschläge für Musterverträge. Die Leitlinien zur Vergütung für die Weitergabe von Daten liegen aber erst als Entwurf vor.
• Beim AI Act liegen Leitlinien zu den Verboten und zu den Transparenzpflichten vor. Die Leitlinien zu Hochrisiko-KI-Systemen hätten bis Februar 2026 vorliegen sollen. Bisher gibt es sie nur als Entwurf.

In der Schweiz arbeitet der Bundesrat ausserdem an einem Cybersicherheitsgesetz nach dem Vorbild des CRA. Geplant sind auch neue Regeln für die künstliche Intelligenz und ein Rahmengesetz für die Sekundärnutzung von Daten. Damit dürften einzelne Vorgaben der EU auch in die Schweizer Gesetzgebung einfliessen. Die Unternehmen sind aber bereits heute betroffen, obwohl die rechtlichen Spielregeln der EU noch nicht vollständig feststehen. Wer jetzt abwartet, riskiert, den Anschluss zu verlieren. Sie sollten deshalb prüfen, welche Vorschriften für Sie gelten und wo Handlungsbedarf besteht. Gerne beraten und unterstützen wir Sie dabei.

TRANSPARENZREGISTER UND NEUE GWG-PFLICHTEN

Claudia Keller Lüthi · Partnerin · Rechtsanwältin · Notarin

Am 1. Oktober 2026 sind gleich zwei einschneidende Erlasse in Kraft getreten: das Bundesgesetz über die Transparenz juristischer Personen (TJPG) und die Revision des Geldwäschereigesetzes (GwG). Beide verfolgen dasselbe Ziel – eine wirksamere Bekämpfung von Geldwäscherei und Terrorismusfinanzierung –, richten sich aber an unterschiedliche Adressatinnen und Adressaten. Wer sich noch nicht damit befasst hat, sollte dies jetzt nachholen: Einzelne Fristen laufen bereits.

DAS NEUE TRANSPARENZREGISTER WER IST BETROFFEN?

Seit dem 1. Oktober 2026 müssen praktisch alle Schweizer Kapitalgesellschaften – AG, GmbH, Genossenschaften, Kommanditaktiengesellschaften sowie gewisse Investmentgesellschaften – ihre wirtschaftlich berechtigten Personen in einem neuen, zentralen Register erfassen. Eine KMU-Ausnahme gibt es nicht: Grösse, Umsatz und Mitarbeiterzahl spielen keine Rolle. Auch ausländische Gesellschaften können meldepflichtig sein - etwa wenn sie eine Zweigniederlassung, die tatsächliche Verwaltung oder Grundeigentum in der Schweiz haben. Ausgenommen von der Meldepflicht sind börsenkotierte Gesellschaften, Vorsorgeeinrichtungen, mehrheitlich staatliche Gesellschaften sowie Vereine und Stiftungen.

HINTERGRUND UND REGISTERZUGRIFF

Aus dem Handelsregister ist die wirtschaftliche Beteiligungsstruktur einer Gesellschaft nicht direkt erkennbar – gerade bei mehrstufigen Strukturen können die wirtschaftliche Eigentümerschaft und der formale Registereintrag auseinanderfallen. Das TJPG soll hier für Transparenz sorgen und es den Behörden ermöglichen, Geldwäscherei und Terrorismusfinanzierung wirkungsvoller zu bekämpfen. Öffentlich einsehbar ist das Register allerdings nicht: Zugriff haben ausschliesslich bestimmte Behörden, etwa Straf- und Polizeibehörden, die Meldestelle für Geldwäscherei und die Grundbuchämter. Geführt wird das Register vom Bundesamt für Justiz. Zugriff erhalten daneben auch dem GwG unterstellte Finanzintermediäre sowie Beraterinnen und Berater, soweit sie die Angaben für die Erfüllung ihrer eigenen Sorgfaltspflichten benötigen – dazu gleich mehr.

WER GILT ALS WIRTSCHAFTLICH BERECHTIGT?

Grundsätzlich gilt als wirtschaftlich berechtigt jede natürliche Person, die eine Gesellschaft direkt oder indirekt kontrolliert – in der Regel ab 25 % Kapitalbeteiligung oder Stimmrechtsanteil. Massgebend ist aber stets die tatsächliche Kontrollmöglichkeit, nicht bloss die formale Quote: Auch ein Vetorecht, das Recht zur Ernennung der Verwaltungsratsmehrheit oder eine Stimmbindung in einem Aktionärsbindungsvertrag können genügen. So zählen beispielsweise auch familiäre Absprachen: Stimmen sich etwa fünf Geschwister mit je 20 % im Familienkreis ab, gelten alle fünf als wirtschaftlich berechtigt. Sind mehrere Aktionäre durch einen Aktionärsbindungsvertrag mit Stimmvereinbarung verbunden und halten sie gemeinsam mindestens 25 % an einer Gesellschaft, gilt zudem jedes Mitglied als wirtschaftlich berechtigt, unabhängig von der individuellen Quote. Lässt sich keine natürliche Person als wirtschaftlich berechtigt identifizieren, gilt ersatzweise das oberste Organmitglied als wirtschaftlich berechtigt – bei der AG die Verwaltungsratspräsidentin, bei der GmbH der Vorsitzende der Geschäftsführung.
Wichtig: Die Definition der wirtschaftlich berechtigten Personen weicht von der bisherigen ab (Art. 697j / 790a OR) und wird – anders als im Geldwäschereigesetz – nicht kaskadenartig, sondern je Kontrollart unabhängig geprüft. Auf das bisherige Aktionärsverzeichnis kann für die Meldung somit nicht einfach zurückgegriffen werden.

MELDUNG UND ZUSTÄNDIGKEIT

Die Gesellschaft identifiziert ihre wirtschaftlich berechtigten Personen, erhebt deren Angaben – Name, Geburtsdatum, Staatsangehörigkeit, Adresse, Art der Kontrolle – und meldet sie elektronisch über die Plattform EasyGov, von wo aus auf das eigentliche Register unter transpareg.admin.ch zugegriffen wird. Verantwortlich für die Identifizierung und Meldung ist das oberste Leitungsorgan. Die Registrierung auf EasyGov ist kostenlos, das Konto muss aber mit der Unternehmens-Identifikationsnummer (UID) verknüpft werden, was mit einem Validierungsprozess von einigen Tagen verbunden ist.

ERLEICHTERUNG BEI EINFACHER STRUKTUR

Für Gesellschaften mit einfacher Struktur gilt eine Erleichterung: Sind alle wirtschaftlich berechtigten Personen bereits als Gesellschafter oder Organpersonen (z. B. Verwaltungsräte) im Handelsregister eingetragen,

kann die Meldung anlässlich einer gleichzeitigen Handelsregistereintragung über das kantonale Handelsregisteramt abgewickelt werden, welches die Daten dann an das Transparenzregister weiterleitet. Zudem genügt in solchen Fällen anstelle einer vollständigen Meldung eine Bestätigung, dass die wirtschaftlich berechtigten Personen bereits im Handelsregister eingetragen sind, ergänzt durch die zusätzlich erforderlichen Angaben.

FRISTEN

Neu gegründete Gesellschaften haben die Meldung innerhalb eines Monats nach dem Handelsregistereintrag vorzunehmen. Für bestehende Gesellschaften gelten gestaffelte Übergangsfristen mit festen Stichtagen: bis 31. Dezember 2026 für ordentlich revisionspflichtige AGs, bis 31. Januar 2027 für andere ordentlich revisionspflichtige Gesellschaften, bis 28. Februar 2027 für nicht ordentlich revisionspflichtige AG und bis 31. März 2027 für die übrigen Gesellschaften sowie ausländische Rechtseinheiten. Sind dagegen bereits alle wirtschaftlich Berechtigten im Handelsregister eingetragen (typischerweise bei der GmbH), gilt die grosszügigste Frist bis 30. September 2028.

Aber Achtung: Unabhängig von diesen Fristen löst jede Handelsregistermutation nach dem 1. Oktober 2026 – etwa ein Wechsel im Verwaltungsrat – sofort eine einmonatige Meldefrist aus. Wer seit Anfang Oktober 2026 bereits eine Mutation vorgenommen hat, sollte prüfen, ob diese Frist bereits läuft oder abgelaufen ist.

Die zeitliche Staffelung wirkt paradox: Je komplexer die Eigentümerstruktur, desto kürzer die Übergangsfrist. Gesellschaften mit vielschichtigen Beteiligungsstrukturen sollten deshalb jetzt das Aktien- bzw. Stammanteilsbuch prüfen, die wirtschaftlich Berechtigten dokumentieren und das EasyGov-Konto einrichten, wenn das noch nicht geschehen ist.

SANKTIONEN

Eine fahrlässige Verletzung der Melde- oder Auskunftspflichten bleibt straflos. Wer sie vorsätzlich verletzt oder der Kontrollstelle falsche Angaben macht – Eventualvorsatz genügt –, riskiert eine Busse von bis zu CHF 500'000.00. Zuständig ist eine beim Eidgenössischen Finanzdepartement angesiedelte Kontrollstelle.

NEU: GWG-PFLICHTEN FÜR BERATERINNEN UND BERATER

Am 1. Oktober 2026 ist auch die Revision des Geldwäschereigesetzes (GwG) in Kraft getreten. Bisher galten die strengen GwG-Sorgfaltspflichten im Wesentlichen für Banken und andere Finanzintermediäre. Neu wird eine eigenständige Kategorie unterstellt: die „Beraterinnen und Berater". Erfasst sind natürliche und juristische Personen, die berufsmässig für Dritte bei finanziellen Transaktionen mitwirken – namentlich bei Immobilientransaktionen, bei der Gründung und Strukturierung von juristischen Personen sowie im Zusammenhang mit Stiftungen und Trusts. Das betrifft je nach Konstellation Treuhänderinnen, Immobilienmakler, Domizilanbieterinnen, Rechtsanwälte oder Notarinnen.

DREI KERNPFLICHTEN

Beraterinnen und Berater treffen drei Kernsorgfaltspflichten: Sie müssen ihre Klientschaft identifizieren und überprüfen, die Geschäftsbeziehung dokumentieren und bei begründetem Geldwäschereiverdacht Meldung erstatten. Hinzu kommt die Pflicht, sich innerhalb von zwei Monaten, also bis Anfang Dezember 2026, einer von der FINMA anerkannten Selbstregulierungsorganisation (SRO) anzuschliessen. Für die Identifikation der beteiligten Klientschaft können sie dabei auch auf das Transparenzregister zugreifen – wobei die blosse Prüfung des Registerauszugs allein der eigenen Sorgfaltspflicht aber nicht genügt; die Angaben sind weiterhin selbst zu verifizieren.

WO AUCH WIR BERATER SEIN KÖNNEN

Für gewisse Tätigkeiten – namentlich Gesellschaftsgründungen und Immobilientransaktionen – können neu auch Anwältinnen und Anwälte sowie Notarinnen und Notare dem GwG unterstehen und verpflichtet sein, sich einer SRO anzuschliessen. Das bedeutet, dass bei entsprechenden Mandaten zusätzliche Sorgfalts-, Identifikations- und Dokumentationspflichten erfüllt werden müssen. Praktisch heisst das: Begleiten wir Sie bei einer dem GwG unterstellten Tätigkeit im Zusammenhang mit einer Firmengründung, Umstrukturierung oder einem Liegenschaftskauf, wird unter Umständen ein zusätzlicher Klärungsbedarf nach Herkunft der Mittel, Zweck der Transaktion und wirtschaftlich Berechtigten bestehen und es kann notwendig sein, zusätzliche Unterlagen einzufordern.

AUSNAHMEN FÜR UNSEREN BERUFSSTAND

Ausgenommen bleiben Tätigkeiten im Zusammenhang mit Gerichts-, Straf-, Verwaltungs- oder Schiedsverfahren – ebenso Transaktionen auf familien-, güter- oder erbrechtlicher Grundlage sowie Schenkungen, da

diese Bereiche typischerweise ein eher tiefes Geldwäschereirisiko aufweisen. Damit besteht nicht in jedem Fall eine Beraterfunktion: Auch ein Grossteil unseres klassischen notariellen Geschäfts – Eheverträge, Erbverträge, Testamente, Schenkungsverträge – fällt von vornherein nicht unter die neuen Pflichten. Die Meldepflicht bei Verdacht greift zudem nur, wenn wir im Namen einer Mandantschaft an einer Finanztransaktion mitwirken und die Information nicht durch das Berufsgeheimnis nach Art. 321 StGB geschützt ist.

WENN SIE SELBST BERATEND TÄTIG SIND

Bieten Sie Dienstleistungen an, die unter die neue Definition fallen könnten – etwa die Gründung und Strukturierung von Gesellschaften für Dritte, die Vermittlung von Immobilientransaktionen oder Trust- und Stiftungsdienstleistungen –, sollten Sie jetzt prüfen, ob Sie selbst dem GwG unterstehen und sich einer SRO anschliessen müssen. Die zweimonatige Frist dafür läuft bereits seit dem 1. Oktober 2026.

FAZIT

Ob Transparenzregister oder GwG-Revision: Beide Neuerungen sind seit dem 1. Oktober 2026 Realität und verlangen von Unternehmen und unter Umständen von Beratenden zusätzliche Sorgfalt und eine weitergehende Dokumentationspflicht. Wer sich noch nicht mit den neuen Pflichten auseinandergesetzt hat, sollte dies jetzt zeitnah nachholen – gerade dort, wo die Übergangsfristen kurz bemessen sind.

In eigener Sache

VERSTÄRKUNG UNSERES TEAMS



Wir freuen uns, dass Vivienne Buzzi seit dem 1. Juli 2026 neu bei uns als juristische Mitarbeiterin tätig ist.

Vivienne Buzzi absolviert bei uns für die Zulassung zur Anwaltsprüfung des Kantons Luzern ein einjähriges Anwaltspraktikum. Sie bringt ihr umfassendes und fundiertes juristisches Fachwissen in sämtlichen Rechtsbereichen in unser Team ein. Zu ihren Aufgaben zählen insbesondere das Verfassen von Rechtsschriften, die Erstellung und Prüfung von Verträgen, die Klärung juristischer Fragestellungen sowie die Korrespondenz mit unseren Mandanten, Behörden und Gegenparteien.

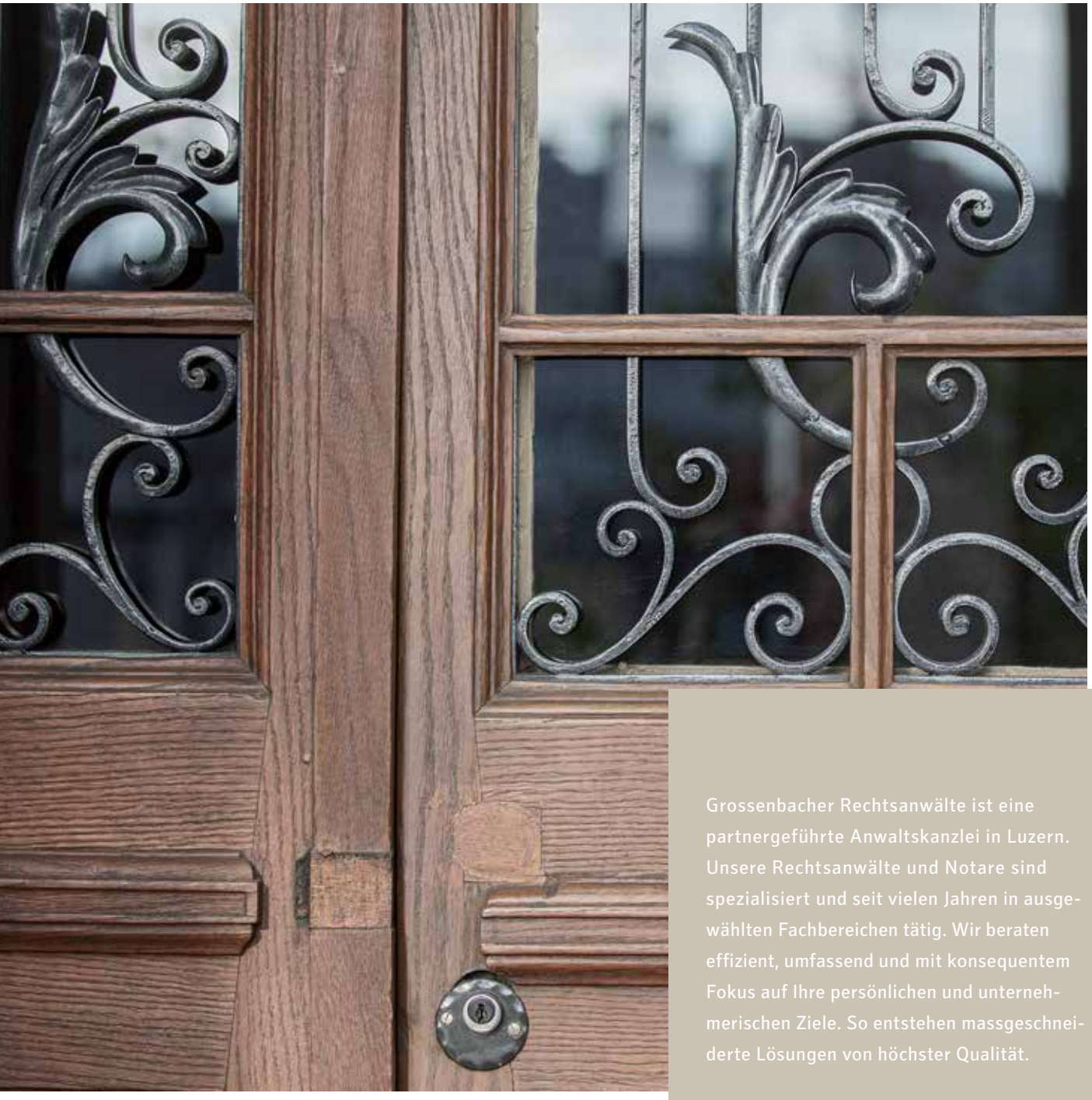
Vivienne Buzzi absolvierte ihr Studium an der rechtswissenschaftlichen Fakultät der Universität Luzern. Den Masterabschluss erwarb sie mit dem Masterprofil „Streiterledigung". Vor ihrer Tätigkeit als juristische Mitarbeiterin in unserer Kanzlei sammelte Vivienne Buzzi praktische Erfahrungen am Bezirksgericht Hochdorf, beim Bezirksgericht Zofingen, am Obergericht Aarau sowie in einer Immobilienunternehmung.

Durch ihre Tätigkeit in unserer Anwaltskanzlei hat Vivienne Buzzi die Möglichkeit, die während des Studiums erworbenen fundierten Fachkenntnisse in der Praxis anzuwenden und sich gleichzeitig optimal auf die Anwaltsprüfung vorbereiten.

Wir heissen Vivienne Buzzi in unserem Team herzlich willkommen.

GROSSENBACHER
RECHTSANWÄLTE

Grossenbacher Rechtsanwälte AG · Zentralstrasse 44
CH-6003 Luzern · +41 41 500 56 56 · www.gr-law.ch



Grossenbacher Rechtsanwälte ist eine partnergeführte Anwaltskanzlei in Luzern. Unsere Rechtsanwälte und Notare sind spezialisiert und seit vielen Jahren in ausgewählten Fachbereichen tätig. Wir beraten effizient, umfassend und mit konsequentem Fokus auf Ihre persönlichen und unternehmerischen Ziele. So entstehen massgeschneiderte Lösungen von höchster Qualität.

Nils Grossenbacher · Partner · Rechtsanwalt · Notar · CAS Real Estate Development
Claudia Keller Lüthi · Partnerin · Rechtsanwältin · Notarin
Christian Leupi · Partner · Rechtsanwalt · MAS Business Information Technology · Mediator SAV
Michael Schumacher · Partner · Rechtsanwalt · Fachanwalt SAV Bau- und Immobilienrecht
Charlène Züger · Rechtsanwältin · Notarin
Thomas Merz · Rechtsanwalt · Notar
Romina Zumbühl · Rechtsanwältin
Sarah Birrer · Rechtsanwältin

Eingetragen im Anwaltsregister