

 <p>Rechtsabteilung der Gruppe W. Kool Foulon Y. Sisowath</p>	E14 RECHTLICH SCHUTZ VON KNOW-HOW UND VERTRAULICHEN INFORMATIONEN (BETRIEBSGEHEIMNISSE)	Seite 1/ 7
		Steuerung Nr.14.4.04 01/2021

Im Rahmen unserer Arbeit sind wir verpflichtet, vertrauliche Informationen zu prüfen und auszutauschen, deren unbefugte Offenlegung den Interessen von VERALLIA schaden und sie beeinträchtigen kann.

Der Zweck dieses Dokuments ist es, Ihnen die Grundlagen und Maßnahmen zu erläutern, die Sie ergreifen müssen, um den Schutz des Know-hows und der vertraulichen Informationen, die sich in Ihrem Besitz befinden oder von Ihnen erzeugt werden, zu gewährleisten.

Sie gilt für alle Mitarbeiter des VERALLIA Konzerns und umfasst alle Funktionen und Aktivitäten.

I DEFINITION VON GESCHÄFTSGEHEIMNISSEN

Um gesetzlich geschützt zu sein, müssen vertrauliche Informationen bestimmte Bedingungen erfüllen und ihr Zugang muss eingeschränkt werden.

(Art. L. 151-1 des französischen Handelsgesetzbuchs oder Richtlinie 216/943 vom 8. Juni 2016, Gesetz zum Schutz von Geschäftsgeheimnissen vom 18.04.2019)

3 kumulative Kriterien, die Informationen müssen:

1	2	3
<p><u>nicht allgemein bekannt oder öffentlich zugänglich sein</u> abzustellen ist auf Personen, die üblicherweise mit dieser Art von Informationen im gleichen Tätigkeitsbereich umgehen</p> 	<p>aufgrund ihrer Geheimhaltung tatsächlich oder potenziell einen <u>kommerziellen Wert</u> haben</p> 	<p>zunter Berücksichtigung der Umstände <u>angemessenen Schutzmaßnahmen</u> durch den rechtmäßigen Eigentümer unterliegen, um sie geheim zu halten.</p> 

Vertrauliche Informationen sind Informationen, die nicht öffentlich bekannt sind und von **denen Personen außerhalb des Unternehmens keine Kenntnis haben sollen**.

Darüber hinaus **ist das nicht patentierte Know-how, das Verallia in jahrelanger Praxis und Erfahrung erworben hat, nur durch Vertraulichkeit geschützt**. Im Falle einer Offenlegung **verliert es seinen Wert** und Verallia kann es nicht mehr als Know-how beanspruchen.

→ **Know-how** umfasst "jede identifizierte und wesentliche Information technischer, industrieller oder kommerzieller Art, die der Öffentlichkeit nicht unmittelbar zugänglich ist und mitgeteilt werden kann."

Beispiele:

Die Zeichnungen der Formen und der Flaschen, die Verallia besitzt, unsere Forschungs- und Entwicklungsprojekte, unsere Produkte, Prozesse oder Technologien, die noch nicht patentiert oder registriert sind.

 Rechtsabteilung der Gruppe W. Kool Foulon Y. Sisowath	E14 RECHTLICH SCHUTZ VON KNOW-HOW UND VERTRAULICHEN INFORMATIONEN (BETRIEBSGEHEIMNISSE)	Seite 2/ 7
		Steuerung Nr.14.4.04 01/2021

Das **Know-how** betrifft nicht nur die eigentliche Herstellung, sondern auch die Vermarktung von Produkten oder Dienstleistungen (z.B. neue, noch nicht registrierte Flaschenmodelle, unsere Geschäftspolitik, unsere strategischen Kundendaten, etc...).

Im Gegensatz zu Know-how umfassen vertrauliche Informationen, die unter den Schutz von Geschäftsgeheimnissen fallen, auch andere Informationen, die sich im weiteren Sinne auf die Strategie des Unternehmens beziehen, wie z. B. Akquisitionen, Finanzierung, strukturelle Entwicklung usw.

II. IDENTIFIZIERUNG, KLASSIFIZIERUNG UND KENNZEICHNUNG VON VERTRAULICHEN INFORMATIONEN UND KNOW-HOW

Der Schutz von vertraulichen Informationen und **Know-how beinhaltet die** Identifizierung, Klassifizierung und vorherige Kennzeichnung von vertraulichen Informationen und Know-how.

1.1. Festlegen des Vertraulichkeitsgrads von Informationen

Tabelle 1: Definieren von Vertraulichkeitsstufen für Informationen

Typ	Verkehr	Ebene
Intern	Zugang innerhalb des Konzerns	1
Vertraulich	Innerhalb des Konzerns auf bestimmte Teams beschränkt	2
Geheimnis	Geheimnis	3

1.2. Einstufung von vertraulichen Informationen und Know-how

Tabelle 2: Datenschutzstufen (auszufüllen von jeder Konzerneinheit und Abteilung)

Stellen Sie sich die folgenden Fragen:

"Kann ich einem Dritten außerhalb des Konzerns den Zugriff auf diese Informationen ermöglichen?"

(Wenn ja, → ist diese Information öffentlich)

"Wenn ein Mitbewerber diese Informationen erhält, verschafft ihnen das einen Vorteil gegenüber uns? »

(wenn ja, → handelt es sich um vertrauliche Informationen)

" Kann ich allen Mitarbeitern freien Zugang zu diesen Informationen gewähren?"

(Wenn ja: Stufe 1)→



Zum Beispiel:

-Wenn die Informationen nur an Mitarbeiter weitergegeben werden sollen, die sie zur Ausführung der ihnen anvertrauten Arbeit benötigen, handelt es sich um Informationen der Stufe 2;

- Das Know-how ist notwendigerweise Level 3.

1.3. Sie müssen in der Lage sein, Know-how und Erfindungen auf eine bestimmte Art und Weise zu datieren und zu bewahren:

Um das Eigentum zu beanspruchen, sind wir verpflichtet zu beweisen, dass das Unternehmen zu einem bestimmten Zeitpunkt das Know-how geschaffen hat oder in dessen Besitz gelangt ist. Daher muss ein Mittel zur Rückverfolgbarkeit und Beweissicherung für den Fall eines Rechtsstreits eingerichtet werden.

Für das **Know-how und die Erfindungen, die noch nicht patentiert sind, wird** dringend empfohlen, eine Einrichtung zu schaffen:

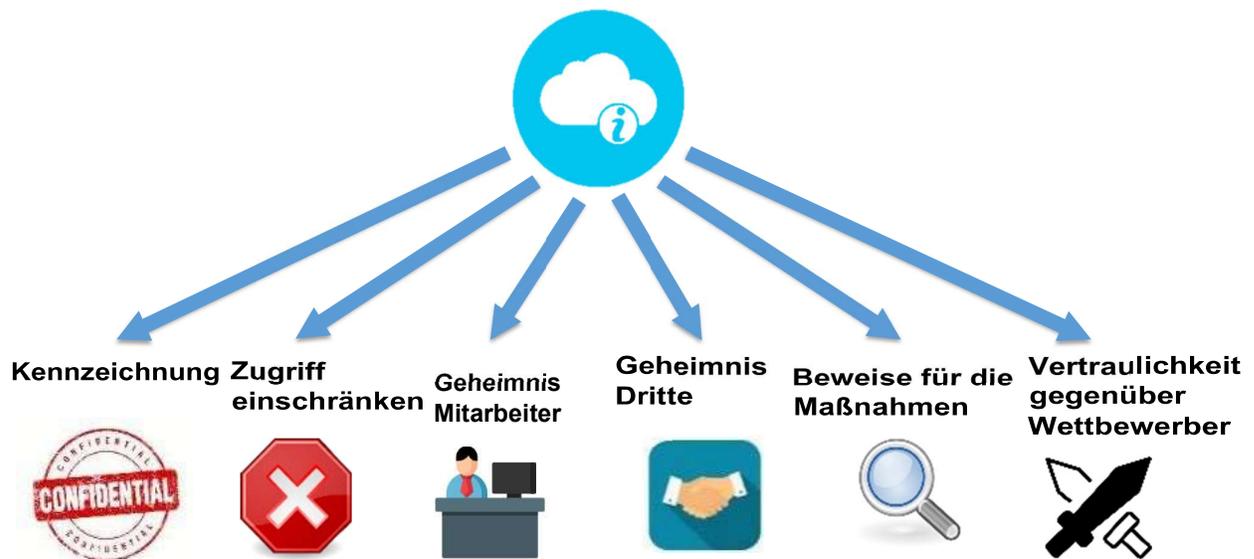
- 1) Labor-Computer, oder wenn das nicht geht

- 2) eine regelmäßige Registrierung (alle 3 oder 6 Monate, abhängig von etwaigen Entwicklungen) der Entwicklungen dieses Know-hows und der vertraulichen Informationen durch soleau-Umschlag (Umschlag, der an geeigneter öffentlicher Stelle hinterlegt wird), private Hinterlegung bei einem Gerichtsvollzieher oder Notar, Versand eines Einschreibens mit Rückschein innerhalb von Verallia, elektronische Zeitstempelung oder digitale Archivierung.

Bitte konsultieren Sie das Verallia IP-Verfahren (auf Teams) für Informationen über das interne Patentanmeldeverfahren.

III. MASSNAHMEN ZUM SCHUTZ VON GESCHÄFTSGEHEIMNISSEN

Um den Schutz des Gesetzes zu genießen, müssen angemessene Maßnahmen zum Schutz unserer vertraulichen oder geheimen Informationen getroffen werden:



Im Falle eines Rechtsstreits mit einem Dritten über die Vertraulichkeit unserer Informationen sind wir verpflichtet, nachzuweisen, dass wir die angemessenen Sicherheits- und Schutzmaßnahmen ergriffen haben.

1. Beschränkung des Zugriffs auf vertrauliche Informationen und Know-How

Für jedes ermittelte **Know-how** muss eine Papier- oder Computerdatei angelegt werden. Diese Datei muss sicher aufbewahrt werden.

- Wenn Sie die Informationen ausgedruckt haben, bewahren Sie sie an einem verschlossenen Ort mit begrenztem Zugang auf.
- Wenn es auf Ihrem Computer gelagert wird, ist es notwendig, Sicherheitsmaßnahmen zu ergreifen (Sicherheitscode, sicherer Server), mit mindestens einem Backup auf einem anderen Server.
- Zugangscodes werden nur an berechnigte Personen weitergegeben und es muss eine Liste der vergebenen Zugänge mit den Namen der Personen aktuell gehalten werden. Bei Austritt ist das Passwort der betreffenden Person sofort zu deaktivieren.
- Für Know-How und vertrauliche Informationen der Stufe 3 müssen Maßnahmen zur Vermeidung der Registrierung oder Vervielfältigung von Dokumenten in Betracht gezogen werden.

 <p>Rechtsabteilung der Gruppe W. Kool Foulon Y. Sisowath</p>	E14 RECHTLICH SCHUTZ VON KNOW-HOW UND VERTRAULICHEN INFORMATIONEN (BETRIEBSGEHEIMNISSE)	Seite 4/ 7
		Steuerung Nr.14.4.04 01/2021

Bei **vertraulichen Informationen** sind die Mitarbeiter für den Schutz der in ihrem Besitz befindlichen vertraulichen Dokumente verantwortlich:

- Identifizierung von Mitarbeitern, die die vertraulichen Daten kennen oder lesen dürfen;
- Beschränken Sie den Zugriff und die Weitergabe von Daten nur auf autorisierte Mitarbeiter
- Vermeiden Sie Drucken,
- Achten Sie beim Drucken auf einem Netzwerkdrucker auf die Ausgabe des Dokuments und lassen Sie die Dokumente nicht in der Nähe des Fotokopierers oder Scanners liegen.
- Vernichten Sie Papierausdrucke nach Gebrauch und setzen Sie auf elektronische Sicherungen,
- Besprechen Sie diese Informationen nur mit Personen, die auf der Liste der zur Vertraulichkeit verpflichteten Personen stehen und die diese Informationen kennen müssen.
- Besprechen Sie diese Themen nicht an öffentlichen Orten (Flugzeuge, Züge, Bahnhöfe, auch nicht in unseren Büros oder im Betriebsrestaurant)
- Lesen Sie vertrauliche Dokumente nicht an einem öffentlichen Ort (Verkehrsmittel, Restaurants, Kongresse usw.) auf Papier oder auf Ihrem Computerbildschirm, es sei denn, Ihr Bildschirm ist durch einen Sichtschutzfilter geschützt
- Achten Sie auf die Liste der Empfänger im E-Mail-Verkehr
- Geben Sie die Vertraulichkeitsstufe bei Bedarf auf Dokumenten oder in E-Mails an (**siehe** E-Mail-Datenschutzverfahren **im Anhang**)
- Zeigen Sie Dokumente, Dashboards, Grafiken, die als vertraulich geltende Informationen enthalten, nicht an öffentlich zugänglichen Stellen an
- Halten Sie alle vertraulichen Dokumente unter Verschluss (Papierdokumente, CDs, USB-Sticks usw.)
- Vergessen Sie nicht, im Falle des Ausscheidens die vertraulichen Unterlagen sinnvoll zu vernichten oder Ihrem Nachfolger oder Ihrem Vorgesetzten anzuvertrauen
- Senden Sie keine vertraulichen Unterlagen an eine externe Person ohne vorherige Freigabe durch den zuständigen Vorgesetzten
- Lassen Sie den Inhalt der Kommunikation vor der weiten Verbreitung von der Hierarchie kontrollieren und validieren (Beispiel: interner Newsletter oder Kunden-Newsletter)
- Senden Sie keine E-Mails mit vertraulichen Informationen von Ihrem persönlichen E-Mail-Posteingang aus, es sei denn, Sie sind ausdrücklich vom Unternehmen dazu autorisiert (ein solcher Vorgang sendet E-Mails ohne den Schutz des VERALLIA-Netzwerks)

2 Vertraulichkeitsvereinbarungen und -klauseln, die eingesetzt werden müssen

Grundsatz: keine Weitergabe von vertraulichen Informationen ohne Geheimhaltungsvereinbarung.

Für vertrauliche Informationen und Know-how der Stufe 3 gilt eine längere Vertraulichkeitsdauer, solange die Informationen nicht öffentlich bekannt werden.

A) Vertraulichkeitsvereinbarungen mit Lieferanten, Anbietern und Beratern:

Lieferanten, Dienstleister, Berater und Zeitarbeitskräfte mit Zugang zu sensiblen Informationen müssen eine Vertraulichkeitsvereinbarung unterzeichnen und sich der geltenden Regeln bewusst sein, bevor sie für den Konzern arbeiten dürfen (Bitte wenden Sie sich an die zuständige Rechtsabteilung).

B) Mit Zeitarbeitskräften: Aushilfskräfte, Praktikanten und Stellvertreter

Ebenso müssen Aushilfskräfte, Zeitarbeiter, Praktikanten und Auszubildende, die in Dienstleistungen involviert sind, die mit vertraulichen Informationen zu tun haben, eine Vertraulichkeitsklausel unterschreiben und sich der geltenden Regeln bewusst sein, bevor sie für den Konzern arbeiten dürfen.

 <p>Rechtsabteilung der Gruppe W. Kool Foulon Y. Sisowath</p>	<p>E14 RECHTLICH</p> <p>SCHUTZ VON KNOW-HOW UND VERTRAULICHEN INFORMATIONEN (BETRIEBSGEHEIMNISSE)</p>	<p>Seite 5/ 7</p> <hr/> <p>Steuerung Nr.14.4.04 01/2021</p>
--	---	---

Besonderes Augenmerk sollte auf ihre Sensibilisierung zu diesem Thema gelegt werden. Der Zugang zu Informationssystemen sollte so weit wie möglich eingeschränkt werden. Die Arbeitszeiten müssen entsprechend den Zeitplänen des Managers festgelegt werden, um diese Mitarbeiter nicht zu lange unbeaufsichtigt zu lassen. Die in den Praktikumsberichten oder Memoranden enthaltenen Informationen müssen vorher vom Abteilungsleiter validiert werden.

C) Mitarbeiter

Schulungen zur Sensibilisierung für den Schutz von vertraulichen Informationen, Know-how und Vertraulichkeitsvereinbarungen müssen von den Mitarbeitern von Verallia absolviert werden. Eine Vertraulichkeitsklausel muss in den Arbeitsvertrag aufgenommen werden (verweisen Sie auf die zuständige Personalabteilung).

Im Falle des Ausscheidens eines Mitarbeiters, der in einem Bereich gearbeitet hat, in dem das Vorhandensein von Know-How oder vertraulichen Informationen der Stufe 3 festgestellt wurde, ist es erforderlich, ihn ein Dokument unterschreiben zu lassen, mit dem er sich verpflichtet, alle in seinem Besitz befindlichen Dokumente zurückzugeben und keine Kopien auf irgendeinem Medium aufzubewahren.

D) Besuche vor Ort:

Jede betriebsfremde Person, die keinen Ausweis hat, der den Zutritt zum Gelände ermöglicht, muss sich je nach Gelände zur Wache oder zum Empfang begeben. Die Identität wird überprüft, sie erhalten einen Ausweis und müssen den Namen und die Funktion der Person angeben, die sie aufsuchen wollte.

Nach der Anmeldung bei der Person, die die Einladung ausgestellt hat, werden die zu befolgenden Sicherheitsanweisungen mitgeteilt und ein Ausweis zum Betreten der Räumlichkeiten ausgehändigt.

In den Fabriken muss jeder Nicht-Verallia-Mitarbeiter von außerhalb, der den Standort besuchen möchte, die Genehmigung des Managements einholen. Es ist verboten, ohne die Erlaubnis des Direktors zu fotografieren oder zu filmen. Begleitpersonen sollten auf die unbefugte Verwendung von Mobiltelefonen (Aufzeichnung eines Gesprächs, eines Videos oder von Fotos) achten.

Für den Zugang zum Forschungs- und Entwicklungszentrum, zur Technischen Direktion und zur Holding-Zentrale in Carpe Diem muss jeder die an diesen Standorten geltenden Zugangs- und Sicherheitsregeln einhalten.

Lassen Sie einen externen Besucher nicht unbeaufsichtigt oder allein in den Räumlichkeiten.

Neben diesem spezifischen Verfahren zum Schutz des Geschäftsgeheimnisses hat die Verallia Gruppe eine Reihe von Verfahren und Regeln eingeführt, die sich gesondert mit der Vertraulichkeit befassen und die einzuhaltenden Grenzen aufzeigen, die im Folgenden aufgeführt sind.

ANHÄNGE

Verallia-Regeln

1. Der Arbeitsvertrag
2. Verallia's Verhaltenskodex (verfügbar auf <https://www.verallia.com/nos-engagements/nos-valeurs>)
3. Die Verallia Charta der internen und externen Kommunikation (verfügbar auf <https://verallia.sharepoint.com/:b:/s/communication/>)
4. Die Verallia-Charta der Nutzer von Computerressourcen und Kommunikationsnetzen (verfügbar auf



Rechtsabteilung der Gruppe
W. Kool Foulon
Y. Sisowath

E14 RECHTLICH

SCHUTZ VON KNOW-HOW UND VERTRAULICHEN INFORMATIONEN (BETRIEBSGEHEIMNISSE)

Seite 6/ 7

Steuerung
Nr.14.4.04
01/2021

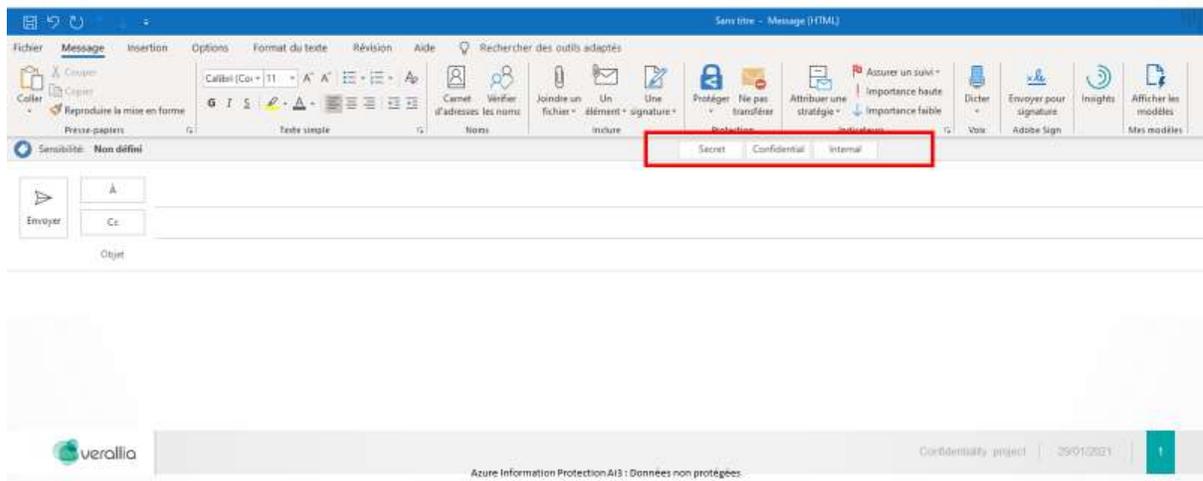
<https://verallia.sharepoint.com/:b/s/doctrine/EXYG1VHbKHNOh99nIYPOAJEB0FvIr9SRocmTck4LnxZgtg?e=Yc5e3O>

5. Verallias Leitfaden für gute Praktiken in den sozialen Medien (verfügbar auf der [speziellen Benutzercharta](#))
6. [Das IP-Verfahren](#) (verfügbar unter <https://verallia.sharepoint.com/:w/s/doctrine/EV8OxkChCidCippP8-07LGMBZk-HhBO787x6L9yqPaOxjA?e=envckr>)

Die Mitgliedschaft in der VERALLIA Gruppe setzt die Einhaltung dieser Regeln sowie dieses Verfahrens voraus.

BEISPIELE FÜR DOKUMENTENSCHUTZ

USE CASE #1: EMAIL PROTECTION



**

USE CASE #2: DOCUMENT PROTECTION

