Der Verantwortliche bestätigt, folgende Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben:

Es wird in jedem Punkt unterschieden, zwischen der lokalen Infrastruktur, sowie der Online Infrastruktur die einen gemieteten V-Server auf Xen Basis bei Domainfactory in Köln bezeichnet.

1. Zugangskontrolle:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Die lokalen Server sind in einem separaten Raum mit eigenem Schließkreis untergebracht und mit einer USV gesichert. Die Switche sind ebenfalls in eigenen abschließbaren Gehäusen untergebracht.

Die eingesetzten Server im Rechenzentrum in Köln sind in einem hochsicheren Rechenzentrum untergebracht.

2. Datenträgerkontrolle:

Alle defekten oder auszutauschenden Medien werden ordnungsgemäße nach DIN 32757 vernichtet, dies bezieht elektronische sowie Papierträger mit personenbezogenen Daten mit ein.

Werden mobile Datenträger eingesetzt, so sind diese mindestens durch eine Softwareverschlüsselung gesichert.

Alle Mitarbeiter sind schriftlich darüber aufgeklärt, keine selbsttätigen Veränderungen an den Datenverarbeitungsanlagen vorzunehmen. Dies betriff explizit auch den Anschuss privater mobiler Datenträger an die EDV.

Das Datacenter in Köln speichert alle Daten verschlüsselt und verfährt ebenfalls nach DIN 32757 mit allen Datenträgern.

3. Benutzerkontrolle:

Alle eingesetzten Systeme verfügen über ein Zugangsberechtigungssystem. Hat eine eingesetzte Software, z.B. die Bildaufbereitung kein eigenes Zugangsberechtigungssystem, so ist sichergestellt, dass der Zugang zur Benutzung der Software bzw. des Betriebssystems reglementiert ist. Die Zentrale Authentifikation und Passwortvergabe für Benutzer- und Computer geschieht im internen Netzwerk über Active-Directory. Das Active-Directory wird immer wieder, spätestens im halbjährlichen Rhythmus überprüft. Ausgeschiedene Mitarbeiter werden sofort gesperrt und nach erneuter Sichtung der Daten gelöscht. Alle Mitarbeiter haben eine Richtlinie zur privaten Internetnutzung erhalten und schriftlich bestätigt.

Der Webshop und das Supportportal sowie das E-Mailsystem werden auf einem V-Server gehostet. Der Dienstleister IT Services mpsna GmbH sorgt per Wartungsvertrag für einen aktuellen Zustand des V-Servers sowie der eingesetzten Software. Alle administrativen Zugänge sind verschlüsselt. Weiterhin sind alle Zugänge über ein Fail-Log-System geschützt. Alle Zugänge zum administrativen Webshop sind durch ausreichend komplexe Passwörter geschützt und werden im jährlichen Rhythmus erneuert. Die Datenbank ist nur lokal erreichbar und gibt keinen Zugriff nach extern Frei.

4. Zugriffskontrolle:

Alle Zugänge, ob Webshop, ERP-System oder Active-Directory werden von der Firma IT Services mpsna GmbH sowie von der Geschäftsführung verwaltet. Zugriffe auf das Active-Directory und den Webshop sowie den V-Server werden protokolliert. Zugänge zu allen Systemen werden über Gruppen konfiguriert. Für alle Mitarbeiter wird eine Zugangsliste gepflegt, diese wird mindestens halbjährlich überprüft.

5. Datenintegrität:

Backupkonzept:

Alle lokalen Server werden durch die Software urBackup täglich im inkrementellen Vollbackup auf ein NAS-Storage LUN gesichert. Wöchentlich, ab Freitag Nacht wird ein aktuelles Vollbackup angelegt. Am Montag wird diese NAS-LUN auf eine von zwei USB-Datenträger gesichert. Diese Mobile Datenträgersicherung werden in den privaten Räumlichkeiten der Geschäftsführer aufbewahrt. Durch die Firma IT Services mpsna GmbH wird sichergestellt, das durch einen Ausfall einer oder mehrerer Infrastruktur Komponenten alleine diese Datensicherung ausreicht um innerhalb von 48 Stunden alle Daten wiederherzustellen.

Der eingesetzte V-Server wird durch ein tägliches, wöchentliches sowie zweiwöchentliches Backup innerhalb des Rechenzentrums gesichert. Hier ist vom maximal Verlust von 24 Stunden auszugehen.

Intern werden weiterhin alle Systeme durch eine professionelle Antiviren Lösung inklusive eines permanenten Forensik-Tools gesichert welches regelmäßig kontrolliert wird. Die Geschäftsführung trägt dafür Sorge, dass alle eingesetzten EDV-Systeme durch die Sicherheitssoftware geschützt sind.

Die extern freigegeben Dienste werden durch ein VPN gesichert und verschlüsselt.

6. Transportkontrolle:

Der Transport vom Webshop bis zur Produktion ist durchgehend verschlüsselt. Der Transport von E-Mail ist soweit es die Gegenstelle anbietet ist ebenfalls verschlüsselt, sofern sich die Partner auf ein System einigen können. Der Abruf von E-Mails ist nur verschlüsselt erlaubt. Hier kommen SSL Zertifikate von Lets-Encrypt zum Einsatz. Diese sind bereits durch die Dienste-Definition immer aktuell, da sie nach max. 8 Wochen ablaufen.

Die Übergabe von Adressdaten zu Versendern wie DPD, Parcel.NL geschieht ebenfalls SSL verschlüsselt.

7. Trennungskontrolle:

Alle erhobenen Daten im Webshop sowie per E-Mail oder mündlich dienen lediglich dem Zweck der Auftragsbearbeitung sowie Buchführung.

Für alle Werbezwecke werden Daten separat durch Zustimmung der Person erhoben und in separaten Datenbanken verwaltet. Es geschieht keine automatische Auswertung der personenbezogenen Daten ohne Zustimmung.

8. Mitarbeiterschulung

Alle Mitarbeiter werden regelmäßig intern zum Umgang mit personenbezogenen Daten, verhalten am EDV Arbeitsplatz sowie zur Passwortsicherheit unterwiesen.