Information sheet: "Technical and organizational measures (TOM) according to Art. 32 (1) GDPR".

Scope / Company:	atrify GmbH
Data Protection Officer (DPO):	Dr. Herwig Pant

Change history			
Ver.	**Date**	**Modified from**	**Change**
0.1	29.06.2021	Director Internal IT/ CISO	Creation of the TOM
0.2	13.07.2021	DPO	Review and comment on the information
0.3	19.01.2022	Director Internal IT/ CISO and Legal Counsel	Finalization of the TOM
0.4	08.08.2022	Legal Counsel	Updating the signature due to the departure of a managing director
0.5	01.09.2022	Director Internal IT/ CISO	Updating of the TOM

Table of contents

1 Preliminary note

Pursuant to Art. 31 (1) of the General Data Protection Regulation (GDPR), all entities that process personal data are required to take technical and organizational measures (TOM) to meet the requirements of the GDPR (formerly the BDSG). The scope of this information sheet "Technical and Organizational Measures (TOM) according to Art. 32 (1) GDPR" is not only geared to the protection of so-called personal data, but also voluntarily applies analogously to the protection of other data / (company) secrets worthy of protection.

2 Measures taken

2.1 Confidentiality (Art. 32 para. 1 lit. b GDPR)

2.1.1 Physical access control

Physical access control is the prevention of unauthorized persons from approaching data processing systems.

2.1.1.1 Structural and technical measures (office building)

	Yes	*No*
• Use of an intrusion detection system:	☒	☐
o Closing contact detector for doors and windows	☐	☒
o Glass breakage sensors	☐	☒
o Motion detectors / light barriers	☐	☒
o Other sensors	☐	☒
• Use of secure doors and windows (laminated safety glass)	☒	☐
• Windows (especially on the first floor) and doors are closed during operating hours	☒	☐
• Rooms are generally locked when not present	☐	☒
• Rooms equipped with PC are locked when not present	☐	☒
• Vehicles in which mobile devices are located are locked	☒	☐
• Sensitive areas of the building are under video surveillance	☒	☐
• Enclosure of the plot	☐	☒
• Protection of building shafts	☐	☒
• Restriction of unhindered access	☒	☐
• Use of separation mechanisms	☐	☒
• Intercom available	☒	☐
• Visual control (visual contact through windows inside doors) available	☒	☐
• Use of a chip card / transponder locking system and/or a locking system with a code lock	☒	☐
• Use of biometric access barriers	☐	☒

2.1.1.2 Organizational measures (office building)

	Yes	*No*
• Gatekeeper service / reception / information as building access control is available:	☐	☒
o Visitors cannot enter the atrify office unnoticed	☒	☐
o Visitors can discreetly describe their concerns (discretion zone)	☐	☒
o Employees at the reception can hold confidential conversations without unauthorized persons listening in	☐	☒
o Documents are protected from access and inspection by unauthorized persons	☒	☐
o Fax machines, printers and monitors are protected from inspection by third parties	☒	☐
o Reception is clearly separated from the waiting area	☐	☒
• Accesses and departures are logged	☐	☒

• Access / exit logs are regularly evaluated	☐	☒
• A separate visitor slip is used for each visitor	☐	☒
• Visitors are picked up and always accompanied	☒	☐
• Obligation to wear authorization badges (for employees)	☒	☐
• Obligation to wear credentials (for visitors)	☒	☐
• Control rounds are carried out	☒	☐
• Central key management and allocation is available	☒	☐
• Access means that have not been issued are documented in an audit-proof manner	☐	☒
• Access authorizations are clearly and unambiguously assigned, including to rooms with distribution boxes	☒	☐
• Access authorizations are regulated in an audit-proof manner in an authorization concept and checked regularly	☒	☐
• Lost access means (transponders, chip cards) are blocked immediately	☒	☐
• Access rights are limited in time	☒	☐
• Security guards / building protection is carefully selected	☒	☐
• Use of security guards / building protection also on weekends and at night	☒	☐
• Cleaning staff is carefully selected	☒	☐
• Server rooms are cleaned only under the supervision of authorized employees	☒	☐
• Criminal investigation consulting services are consulted on building security	☐	☒

2.1.1.3 Structural and technical measures (data center)

	Yes	***No***
• Use of an intrusion detection system:	☒	☐
o Closing contact detector for doors and windows	☒	☐
o Glass breakage sensors	☒	☐
o Motion detectors / light barriers	☒	☐
o Other sensors	☒	☐
• Use of secure doors	☒	☐
• All areas of the building are under video surveillance	☒	☐
• Enclosure of the plot	☒	☐
• Protection of building shafts	☒	☐
• Restriction of unhindered access	☒	☐
• Use of separation mechanisms	☒	☐
• Intercom available	☒	☐
• Visual control (visual contact through windows inside doors) available	☒	☐

• Use of a chip card / transponder locking system and/or a locking system with a code lock	☒	☐
• Access only for operational employees who have been previously authorized via an identity check.	☒	☐

2.1.1.4 Organizational measures (data center)

	Yes	*No*
• Gatekeeper service / reception / information as building access control is available:	☒	☐
o Visitors cannot enter the building unnoticed	☒	☐
• Accesses and departures are logged	☒	☐
• Access / exit logs are regularly evaluated	☒	☐
• Employees are picked up and always accompanied by security personnel	☒	☐
• Obligation to wear authorization badges (for employees)	☒	☐
• Control rounds are carried out	☒	☐
• Central key management and allocation is available	☒	☐
• Access means that have not been issued are documented in an audit-proof manner	☒	☐
• Access authorizations are clearly and unambiguously assigned, including to rooms with distribution boxes	☒	☐
• Access authorizations are regulated in an audit-proof manner in an authorization concept and checked regularly	☒	☐
• Lost access means (transponders, chip cards) are blocked immediately	☒	☐
• Access rights are limited in time	☒	☐
• Security guards / building protection is carefully selected	☒	☐
• Deployment of security guards / building protection 24/7	☒	☐
• Criminal police advisory services are consulted on building security	☒	☐

2.1.2 Admission control

Admission control is the prevention of unauthorized persons from entering data processing systems with which personal data are processed or used.

2.1.2.1 Technical measures

	Yes	*No*
• Security requirements for information systems / IT systems (incl. mobile devices) are precisely determined and the systems are configured accordingly	☒	☐
• Login to IT systems is done with username and password:	☒	☐

o Preventing the selection of very weak passwords	☒	☐
o Strong passwords even on internal systems	☒	☐
o 2-factor authentication	☒	☐
• Logon to IT systems takes place with chip cards	☐	☒
• Logon to IT systems takes place with biometric features	☐	☒
• Password quality is technically checked	☒	☐
• Use of password management	☒	☐
• Failed login attempts activate a lockout mechanism	☒	☐
• Validity period of access authorizations is limited	☒	☐
• Encryption of IT systems (incl. mobile devices)	☒	☐
• Encryption of data carriers (e.g. USB sticks, external hard disks)	☒	☐
• The taking along of official devices and data carriers is regulated	☒	☐
• Use of an intrusion detection system	☒	☐
• Password protected screen lock	☒	☐
• Access data is transferred securely during remote accesses	☒	☐
• Lost access means (transponders, chip cards) are blocked immediately	☒	☐
• Firewall:	☒	☐
o Central / server-side deployment of a hardware and software firewall to seal off all Internet-enabled devices from the Internet	☒	☐
o Local deployment of software firewalls	☒	☐
o Use of firewalls also at application level	☒	☐
o Proper configuration of the firewall are regularly checked	☒	☐
o Monitoring of the firewall to detect access attempts	☒	☐
• Centralized / server-side deployment of anti-virus software	☒	☐
• Local deployment of antivirus software	☒	☐
• Antivirus software for mobile devices	☒	☐
• No remote desktop access (RDP-TCP ports) open	☒	☐
• Remote desktop access (RDP-TCP ports) over the Internet is minimized and secured for remote access to PCs and running applications	☒	☐
• No use of WLAN	☐	☒
• WLAN is secured by encryption incl. 802.1X authentication	☒	☐
• Use of two- or multi-factor authentication:	☒	☐
o Encrypted VPN connections are secured with two-factor authentication	☒	☐
o Two-factor security for administrator access - at least for Internet services	☒	☐

o Tokens / smart cards are used by default to log on to IT systems	☒	☐
• Deployment of Mobile Device Management (MDM) / Enterprise Mobility Management (EMM)	☒	☐
• Possibility of remote deletion of smartphones / mobile devices	☒	☐
• Logins to IT systems are logged	☒	☐
• PC cases are locked	☐	☒
• Printers and fax machines are protected from unauthorized access	☒	☐

2.1.2.2 Organizational measures

	Yes	***No***
• Information systems / IT systems (incl. mobile end devices) are regularly checked for compliance with security requirements	☒	☐
• Deployment of Identity and Access Management (IAM)	☒	☐
• Password protection:	☒	☐
o Password policy is effectively in place	☒	☐
o Employees are aware of what strong passwords are and how to handle them. Requirements of ISO 27001 are met.	☒	☐
o Blocking and reassignment of passwords after an incident is regulated	☒	☐
• IT security policy is effectively implemented	☒	☐
• Teleworking / mobile office / home office is regulated	☒	☐
• Access authorizations are assigned clearly and unambiguously	☒	☐
• Access authorizations and their validity periods are regulated in an audit-proof manner in an authorization concept and regularly checked	☒	☐
• Log files are regularly evaluated to identify misuse of access authorizations	☒	☐
• Electronic access means (transponder / chip card) are managed and assigned centrally	☒	☐
• Employees are instructed to lock screens during PC absence	☒	☐
• Screens are not visible to third parties	☒	☐
• Guideline for the use of operational DP devices / IT systems is effectively in place	☒	☐
• Printers, copiers and fax machines are placed in a suitable location	☒	☐
• Mobile devices are stored in an appropriate manner	☒	☐
• Firewall:	☒	☐

o Use of qualified personnel / service provider to configure the firewall	☒	☐

2.1.3 Access (authentication) control

Access (authentication) control ensures that only corrected users of data processing systems can view, use, or process the data that is required for your specific task performance and for which you have been granted authorization.

2.1.3.1 Technical measures

	Yes	*No*
• Use of a central directory service	☒	☐
• Use of antivirus software	☒	☐
• Encryption of files and folders	☐	☒
• Encryption of servers and databases	☐	☒
• Files and folders are password protected	☒	☐
• Access events are logged, including failed access attempts	☒	☐
• Query options of databases are limited	☒	☐
• Access rights to necessary resources and peripherals in the network are restricted	☒	☐
• Unauthorized computers and end devices on the network are rejected	☒	☐
• Unauthorized (mobile) storage media are rejected	☒	☐
• Customer profiles are managed in parallel and separately on the software side	☒	☐
• Unnecessary security-relevant programs and functions (e.g. apps) are uninstalled / deactivated	☒	☐
• Home Office:		
o Encrypted VPN connection in conjunction with two-factor authentication	☒	☐
• Remote maintenance:		
o Remote maintenance access is limited only to the specific systems to be maintained instead of to complete network segments, if necessary additionally secured by so-called "jump servers".	☒	☐
o Remote maintenance access is only enabled for specific purposes and for a limited period of time	☒	☐
o Transfer of files is disabled if they are not required for remote maintenance	☒	☐
o Remote maintenance accesses are fully logged	☒	☐
o Logs for remote maintenance are regularly evaluated	☒	☐
o Encryption of the transport path for remote access (VPN / TLS)	☒	☐

o Remote maintenance accesses are blocked / prevented after termination of a service contract	☒	☐
• Administration:		
o Lockable file cabinets are available and are locked at the end of the working day	☒	☐
o "Old files" are kept inaccessible to unauthorized persons	☒	☐
o Cleaning personnel cannot access sensitive data	☒	☐
o Data is processed exclusively on authorized hardware and software	☒	☐

2.1.3.2 Organizational measures

	Yes	***No***
• Deployment of Identity and Access Management (IAM)	☒	☐
• Authorizations for users and administrators are assigned in a differentiated manner	☒	☐
• Access authorizations and their validity periods are regulated in an authorization concept (profiles / roles) in an audit-proof manner, documented and regularly checked by an independent auditor.	☒	☐
• Differentiated folder concept available for uniform and comprehensible naming and storage	☒	☐
• Storage media are clearly labeled and securely stored	☒	☐
• Secure data media storage, management and disposal	☒	☐
• Storage media and drives are not reused, but physically destroyed	☒	☐
• Storage media and drives are securely and completely erased	☒	☐
• Destructions of data carriers are documented with destruction receipts	☒	☐
• Activities of the system administrator are logged	☒	☐
• Clear Desk / Clean Screen / Order in the workplace is effectively implemented	☒	☐
• Home Office:	☒	☐
o Overview of employees for whom home office work is generally possible	☒	☐
o Overview of employees who currently work in the home office	☒	☐
o Overview of data-processing devices used by employees in the home office	☒	☐
o Employees in the home office can be reached via various communication channels in the event of an incident	☒	☐
o Use of private end devices in exceptional cases is regulated	☒	☐
o Employees are made aware of how to use video conferencing tools	☒	☐
o Carrying and disposal of sensitive paper documents is regulated	☒	☐

2.1.4 Separate processing (separation control)

The aim of separate processing is to ensure the purpose limitation of personal data and the prevention of misuse.

2.1.4.1 Technical measures

	Yes	*No*
• Use of a central directory service	☒	☐
• Database queries / free query languages (especially SQL) are restricted	☒	☐
• Development and production system are separated	☒	☐
• Customer profiles are managed in parallel and separately on the software side	☒	☐
• Encryption is performed on a customer-specific basis	☒	☐
• Cryptographic keys serve only one purpose	☒	☐
• Data is stored logically or physically separated	☐	☒
• System environments on which services are offered to customers are separated virtually or physically	☐	☒
• Mapping tables for pseudonymized data are separated from them and kept on a separate, secured system	☒	☐
• Partitions for operating systems and data are separated	☐	☒
• Networks are separated (network segmentation):	☒	☐
o Internet servers are operated in a so-called "demilitarized zone" (DMZ)	☒	☐
o Logging at firewall level to detect and analyze even unauthorized access between networks	☒	☐
o IT administrators are automatically notified when unauthorized processing is suspected	☒	☐

2.1.4.2 Organizational measures

	Yes	*No*
• Databases are documented in detail	☒	☐
• Business departments and IT department are separated from each other according to function / tasks	☒	☐
• New data processing procedures and significant changes to legacy procedures go through a formalized approval process	☒	☐
• Database authorizations are regulated and documented in an audit-proof manner in an authorization concept	☒	☐
• Data records are provided with purpose attributes	☒	☐
• Data sets that are processed for the same purpose are encrypted	☐	☒

• Networks are separated (network segmentation):	☒	☐
o Process for proper configuration of the firewalls and their regular check is regulated	☒	☐

2.1.5 Pseudonymization (Art. 32 para. 1 lit. a GDPR; Art. 25 para. 1 GDPR)

The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the addition of further information.

2.1.5.1 Technical measures

	Yes	*No*
• Pseudonyms are used in secondary systems that are used for strategic data analysis and decision support	☒	☐
• Pseudonyms are used when creating test data	☒	☐
• Pseudonyms are used in sub-processes of business processes where the original data is not required:	☒	☐
o Person-identifying data are specified to be replaced by pseudonymization	☐	☒
o Pseudonymization rules are defined, possibly linked to personnel or customer identification numbers	☐	☒
o Employees are defined who are authorized to manage the pseudonymization procedures, to perform pseudonymization and, if necessary, to perform depseudonymization	☒	☐
o Permissible occasions for pseudonymization and de-pseudonymization processes are specified	☒	☐
o Mapping tables or the secret parameters that go into an algorithmic pseudonymization are randomly generated	☒	☐
o Assignment tables or secret parameters are protected / stored in a separate and secured system against both unauthorized access and unauthorized use.	☒	☐
o Pseudonymized data is separated from the personal identifying data to be replaced	☒	☐

2.1.5.2 Organizational measures

	Yes	*No*
• Personal data is anonymized / pseudonymized in case of disclosure	☒	☐
• Personal data is anonymized / pseudonymized after expiry of the retention period	☒	☐

2.2 Integrity (Art. 32 para. 1 lit. b GDPR)

2.2.1 Transfer control

Transfer control means the control of transmission and transport of personal data as well as the control of storage of data on data carriers.

2.2.1.1 Technical measures

	Yes	*No*
• Encryption of the VPN connection	☒	☐
• Data is provided via SFTP / HTTPS	☒	☐
• Encryption of data carriers	☒	☐
• Encryption of mobile devices	☒	☐
• Encryption of databases	☒	☐
• Data encryption	☒	☐
• Suitable cryptographic methods with algorithms established in the professional world are selected	☒	☐
• Use of appropriate key management for cryptographic keys with suitable key generators in a secure environment	☒	☐
• Use of password management	☒	☐
• Authenticity of transmitted data is ensured by signature procedure	☒	☐
• Personal data is passed on anonymized or pseudonymized	☒	☐
• Changes / manipulations of transmitted data subsequently detectable	☒	☐
• Data carriers are scanned for malware infestation	☒	☐
• Storage media and drives are securely erased or physically destroyed (e.g. shredding) without leaving any residue before being reused:	☒	☐
o Deletion procedures are established	☒	☐
• Deployment of Mobile Device Management (MDM) / Enterprise Mobility Management (EMM)	☒	☐
• Accesses, transmissions and retrievals are logged / recorded	☒	☐
• Printer queue is only processed after personal login at the printer	☒	☐
• Data memories of printers / copiers / multifunction devices are securely erased or physically destroyed without leaving any residue before disposal	☒	☐
• Use of document shredders (security level P-3 / P-4 / P-5, cross-cut)	☒	☐
• Email Security:	☒	☐
o Encryption of the transport route of e-mails (SSL / TLS)	☒	☐
o End-to-end email encryption (E2EE)	☐	☒
o Emails are displayed in "text only" format	☐	☒

o Links in e-mails are checked before the e-mails are called	☒	☐
o Incoming emails are scanned for malware	☒	☐
o Dangerous attachments are blocked	☒	☐
o Flat rate forwarding rules for cloud hosting is disabled	☒	☐

2.2.1.2 Organizational measures

	Yes	*No*
• Logged transmission, access and retrieval data are evaluated by an independent auditor on a regular / occasion-related basis	☒	☐
• Actions are defined when weaknesses in key lengths and encryption methods or products are discovered	☒	☐
• Backup copies / backups are handled carefully and in a regulated manner	☒	☐
• Disk directory is maintained	☐	☒
• Emails are not forwarded to employees' private email accounts	☒	☐
• Data is processed exclusively on authorized hardware and software	☒	☐
• Use of mobile data carriers is regulated	☒	☐
• Email Security:	☒	☐
o Employees are made aware of the dangers of encrypted email attachments	☒	☐
o Employees are informed at least annually about current attack variants	☒	☐
o Employees are sensitized to recognize fake e-mails	☒	☐
• Commissioning of reliable transport companies:	☒	☐
o External service providers with possible access to data are obligated to maintain data protection	☒	☐
o Transport routes are documented	☒	☐
o Storage location and data carrier are documented	☒	☐
o Duration of the transfer is documented	☒	☐
o Personal information is removed from file metadata	☒	☐
o Taking of containers from protected areas is logged	☒	☐
o Bags are checked randomly	☐	☒
o Suitable packaging of data carriers, which excludes damage as far as possible	☒	☐
o Verification procedure for the dispatch and receipt of data-carrying consignments is implemented	☒	☐
o Backup copies of data carriers are created that are to be transported	☒	☐

	o Authorizations for sending, forwarding and receiving data media are clearly and unambiguously assigned	☒	☐
	o Data carriers are clearly marked with regard to sender and recipient	☒	☐
	o Transport containers are clearly and unambiguously labeled to avoid confusion	☒	☐
	o Shipping is carried out by carefully selected and trusted personnel	☒	☐
	o The type of transport and the transport service used are determined depending on the sensitivity of the transported data	☒	☐
	o Transport routes and means of transport are specified	☒	☐
	o Use of lockable / sealed / sealed and stable transport containers.	☒	☐
	o Knowledge of the transporter about the transported data is avoided	☒	☐
	o In case of regular data carrier exchange with a recipient, the same data carriers are used	☒	☐
	o Data carriers are checked before transport with regard to the non-reconstructability of deleted data sets that are not to be transmitted	☒	☐
	o Data carrier input or output book is kept	☒	☐

2.2.2 Input control

Input control is understood to mean the subsequent verification of "who - when - viewed, entered, modified, transmitted or deleted - in what manner - what personal data".

2.2.2.1 Technical measures

	Yes	***No***
• Use of a log management (logging and log evaluation system)	☒	☐
• Entries, changes and deletions of data by individual user names are monitored and logged	☒	☐
• Changes to applications and IT systems are monitored and logged	☒	☐
• Entries in log files or tables are automatically logged in an audit-proof manner	☒	☐
• Activities of the (system) administrators are logged	☒	☐
• Changes / manipulations of stored data are subsequently detectable (e.g. signature procedure, checksum procedure)	☒	☐
• Log files / logs are stored securely by the system	☒	☐

2.2.2.2 Organizational measures

	Yes	*No*
• Logging concept is effectively implemented	☒	☐
• Log files are evaluated by a system administrator / independent auditor on a regular / ad hoc, manual / automated basis	☒	☐
• Log files are evaluated according to the dual control principle	☐	☒
• Deployment of Identity and Access Management (IAM)	☒	☐
• Authorizations for users and administrators are assigned in a differentiated manner	☒	☐
• Access authorizations and their validity periods are regulated in an authorization concept (profiles / roles) in an audit-proof manner, documented and regularly checked by an independent auditor.	☒	☐
• Overview of the personal data to be processed is available	☒	☐
• Overview of the software is available, by means of which data can be entered, modified and deleted	☒	☐
• Data fields are checked for plausibility if they make sense	☒	☐
• Log files / logs are deleted in due time	☒	☐
• Deletion concept is effectively implemented	☒	☐
• Deletion routines with clear responsibilities for manual and digital data are effectively implemented	☒	☐

2.3 Availability and resilience (Art. 32 para. 1 lit. b GDPR)

2.3.1 Availability control and rapid recoverability (Art. 32(1)(c) GDPR)

Availability control is the protection against data loss and destruction and the simultaneous possibility of recovery when needed.

2.3.1.1 Technical measures

	Yes	*No*
• Firewall:	☒	☐
o Central / server-side deployment of a hardware and software firewall to seal off all Internet-enabled devices from the Internet	☒	☐
o Local deployment of software firewalls	☒	☐
o Use of firewalls also at application level	☒	☐
o Proper configuration of the firewall are regularly checked	☒	☐
o Monitoring of the firewall to detect access attempts	☒	☐
• Centralized / server-side deployment of anti-virus software	☒	☐

• Local deployment of antivirus software	☒	☐
• Antivirus software for mobile devices	☒	☐
• No remote desktop access (RDP-TCP ports) open	☒	☐
• Remote desktop access (RDP-TCP ports) over the Internet is minimized and secured for remote access to PCs and running applications	☒	☐
• Use of web filters	☒	☐
• Security-relevant networks, IT systems, applications and other IT components are regularly maintained and updated	☒	☐
• New software is installed and configured in a controlled manner by the IT department	☒	☐
• Faults can be identified by remote display	☒	☐
• IT infrastructure (network, storage, server, clients) is available redundantly	☒	☐
• Hard disk mirroring (RAID system) is implemented	☒	☐
• Remote maintenance is implemented securely	☒	☐
• Fire and smoke detection systems available	☒	☐
• Privacy vault available	☒	☐
• Partitions for operating systems and data are separated	☐	☒
• Sufficient protective measures in the server room:	☒	☐
o Local uninterruptible power supply (UPS) and emergency power supply available	☒	☐
o Overvoltage protection available	☒	☐
o Server room is located above the water line (relevant especially for flood areas)	☒	☐
o No sanitary connections in or above the server room	☒	☐
o Video surveillance available	☒	☐
o An alarm is triggered in the event of unauthorized access	☒	☐
o Air conditioner available	☒	☐
o Temperature and humidity is monitored	☒	☐
o Fire protection measures (including fire extinguishers) are effectively implemented	☒	☐
o Protection against water and moisture damage present	☒	☐
• Patch management / update management is operated:	☒	☐
o Exclusive use of desktop operating systems for which security updates continue to be provided	☒	☐
o Desktop operating systems are updated automatically	☒	☐
• Malware protection:	☒	☐
o Endpoint Data Protection / Endpoint Security is implemented	☒	☐

o Antivirus signatures are automatically updated daily	☒	☐
o Alarm messages are recorded centrally by the IT department	☒	☐
o Use of antivirus solution with local heuristic detection configured as "high".	☒	☐
o Use of sandboxing procedures or Advanced Endpoint Detection and Response (EDR) only under strict consideration of data protection regulations	☒	☐
• Ransomware Protection:	☒	☐
o Macros in Office documents are largely dispensed with in day-to-day operations	☒	☐
o Only signed Microsoft Office macros are allowed	☒	☐
o Automatic execution of downloaded programs is prevented	☒	☐
o Windows Script Hosts (WSH) on clients is disabled	☒	☐
o Checking whether the restriction of Powershell scripts with the "ConstrainedLanguageMode" to Windows clients is reasonably feasible	☒	☐
o Use of a web proxy server with (daily) up-to-date blocking lists of malicious code download sites (IOCs)	☐	☒
• Backup:	☒	☐
o Backup media is stored in a suitable and physically secure manner	☒	☐
o Backup copies / backups of data, process states, configurations, data structures, transaction histories and non-networked systems are made regularly	☒	☐
o Backup copies / backups are encrypted	☒	☐

2.3.1.2 Organizational measures

	Yes	***No***
• Central and uniform procurement strategy for hardware and software is implemented	☒	☐
• Passwords are stored suitably and securely	☒	☐
• Third-party software is tested before introduction	☒	☐
• Networks, IT systems, applications, other IT components and procedures to ensure person-independent IT operations are documented	☒	☐
• Service instructions and security guidelines for data backup are effectively implemented	☒	☐
• Contingency:	☒	☐

o Emergency concept is implemented effectively and is tangible in paper form for the relevant groups of people	☒	☐
o Up-to-dateness of the emergency concept is checked regularly	☒	☐
o Resumption of operations is made possible by various pre-planned and pre-tested sequence steps in the emergency plan	☒	☐
o Restart scenarios are regularly rehearsed	☒	☐
o Competent authorities and notification obligations are specified in the emergency plan	☒	☐
o Emergency reserve hardware available to compensate for failures	☒	☐
o Alternative rooms and infrastructures available in the event of a disaster	☒	☐
o Rapid development of a fallback infrastructure is possible	☒	☐
o Well-structured and up-to-date network plan available	☒	☐
o Security and data incident detection and reporting process in place	☒	☐
o Employees are informed about contact persons in case of security incidents	☒	☐
o Availability of contact persons in case of security incidents is guaranteed	☒	☐
o Central administration access data and access options are stored securely in case of emergency	☒	☐
• IT administrators:	☒	☐
o Administrators also use non-privileged default accounts for other non-administrative work	☒	☐
o Regulation is effectively implemented that administrators do not surf the Internet or read / send e-mails with administrator rights	☒	☐
o Very strong passwords for local admin accounts available	☒	☐
o Consistent use of two-factor authentication procedures for applications, as far as possible	☒	☐
o Entire operation is not dependent on individual administrators	☒	☐
o Sufficient personnel resources available in the IT department	☒	☐
o Substitution arrangements for administrators in place	☒	☐
o In case of failure of several administrators, it is ensured that the working ability of the operation can be maintained	☒	☐
o Fast and regulated accessibility of administrators is ensured	☒	☐
• Patch management / update management is operated:	☒	☐
o Patch management concept with update plan is effectively implemented	☒	☐

o Information on security vulnerabilities of the hardware and software used is regularly evaluated	☒	☐
o Security updates for the server are applied in a timely manner.	☒	☐
o Regulated / automatic process for browser updates available	☒	☐
o Regulated / automatic process for updates of basic components (e.g. Java, PDF reader) available	☒	☐
• Malware protection:	☒	☐
o Internal instruction to employees on how to deal with alarm messages is effectively implemented	☒	☐
o Sequence plan in the event of a malware attack is available in the IT department	☒	☐
• Ransomware Protection:	☒	☐
o Employees are informed about risks of macro activation at least annually	☒	☐
o Emergency plan for dealing with encryption Trojans is available on paper	☒	☐
o Backup and recovery strategy ensures backups cannot be encrypted by ransomware	☒	☐
• Data backup concept is effectively implemented	☒	☐
• Backup copies / backups are kept separately	☒	☐
• Backup copies / backups are stored in a secure location outside the server room	☒	☐
• Backup:	☒	☐
o Backup copies / backups are performed according to the 3-2-1 rule	☒	☐
o Backup and restart concept in place	☒	☐
o Regular tests to ensure that all relevant data is included in the backup process, recoverability is working and results are logged	☒	☐
o At least one backup system is unencryptable by ransomware	☒	☐

2.4 Procedures for regular review, assessment and evaluation (Art. 32(1)(d) GDPR; Art. 25(1) GDPR)

2.4.1 Order control

Order control is understood to mean the processing of personal data on behalf of a third party and according to the instructions of the client (Art. 28 GDPR). The responsibility remains with the client. In the event of a data transfer to a third country, additional provisions must be met in order to ensure a consistently adequate level of protection (Art. 44-49 GDPR).

	Yes	No
• Clear contract design in accordance with Art. 28 GDPR in place	☒	☐
• Orders are placed in a formalized manner (order form)	☒	☐
• Place of processing is determined	☒	☐
• Checking whether commissioned processing is permissible	☒	☐
• Contracts and agreements are concluded in writing	☒	☐
• TOM of the contractor are checked before the start of processing	☒	☐
• Competencies and duties between client and contractor are clearly delineated	☒	☐
• Contractors and subcontractors have appointed a proper data protection officer	☒	☐
• Contractors are carefully selected according to the level of their technical and organizational measures	☒	☐
• Contractors are audited on an ongoing basis	☒	☐
• Safety measures are defined, which the contractor has to implement	☒	☐
• Reporting requirements are defined	☒	☐
• Rules of conduct in the event of malfunctions are defined	☒	☐
• Processing is only carried out according to instructions documented in writing	☒	☐
• Proper fulfillment of the contract by the contractor is controlled (data protection audit)	☒	☐
• Contractors assist in responding to requests from affected parties	☒	☐
• Contractor support for violations to be reported	☒	☐
• The complete deletion / return of the data after completion of the order is ensured	☒	☐
• Standardized AV review process for external data processing is implemented	☒	☐
• Contractor support regarding the security of processing	☒	☐
• Contractors assist with data protection impact assessment and prior consultation with the supervisory authority	☒	☐
• Notification obligations of the contractors in the event of measures taken by the supervisory authority or in the event of investigations are specified	☒	☐
• Effective possibilities for control are granted within the framework of the contract, as well as obligations of the contractor to tolerate and cooperate	☒	☐
• Sanctions for breach of contract are established	☐	☒
• Modalities of handover and transport of data are defined	☐	☒
• Security class of the data to be processed in the order is defined	☐	☒
• Subcontracting relationships are defined	☒	☐

• Subcontractors are required to comply with the Contractor's data protection obligations	☒	☐
• Liability of the contractor for compliance with the data protection obligations of the subcontractor is regulated	☒	☐
• Contractor notification requirements regarding intended changes are established when changes are generally approved	☒	☐
• Client's right to object to planned subcontractors is established when they are approved in general	☒	☐
• Employees of contractors are obliged to confidentiality and	☒	☐
• Standard contractual clauses with recipients outside the EU/EEA are concluded	☒	☐

2.4.2 Data Protection Management

Data Protection Management (DPM) is a controlled and managed process over the life cycle of processing activities. It aims to implement legal and operational requirements of data protection.

2.4.2.1 Technical measures

	Yes	*No*
• Use of software solutions for data protection management	☒	☐

2.4.2.2 Organizational measures

	Yes	*No*
• Binding safety guidelines in place	☒	☐
• (IT) security concept is effectively implemented and regularly reviewed	☒	☐
• Vulnerability analyses in IT are carried out on a regular basis	☒	☐
• Directive on the use of e-mail and the Internet is effectively implemented	☒	☐
• Social media policy is effectively implemented	☒	☐
• Directive on video surveillance is effectively implemented	☒	☐
• Time recording policy is effectively implemented	☐	☒
• Directive on tracking systems in fleet vehicles effectively implemented	☒	☐
• Data protection policy / data protection concept is effectively implemented	☒	☐
• Responsibilities for information security management are defined	☒	☐
• Human safety factor:	☒	☐
o Employees are trained and sensitized at least annually	☒	☐

o Employees are sensitized regarding current and frequent cyber attacks	☒	☐
o New employees are consistently instructed on the proper handling of IT components and on how to behave in the event of social engineering attacks	☒	☐
o New employees are sensitized regarding IT risks before starting data processing (also for temporary staff)	☒	☐
o Processes of social engineering attacks are presented to employees to raise awareness	☒	☐
o Employees are informed about reporting channels and responsibilities	☒	☐
• Procedure for entry / exit will be present	☒	☐
• Disk directory is maintained	☒	☐
• Employees are committed to confidentiality	☒	☐
• Clear Desk and Clear Screen policy are effectively implemented	☒	☐
• Information requirements are implemented	☒	☐
• Formal process in place for handling stakeholder inquiries	☒	☐
• Visitor policy is effectively implemented	☒	☐
• Whistleblowing directive / whistleblower system effectively implemented	☐	☒
• Register of processing activities for controllers in place and audited at least annually	☒	☐
• Directory of processing activities for processors in place and audited at least annually	☒	☐
• Policy on remote maintenance by own employees is effectively implemented	☒	☐
• Directive on teleworking / mobile office / home office is effectively implemented	☒	☐
• Directive on the transfer and use of mobile devices is effectively implemented	☒	☐
• Risk analyses are carried out and a protection level concept is effectively implemented	☒	☐
• Logging concept is effectively implemented	☒	☐
• Reporting process for emerging vulnerabilities and other risk factors is in place and risk analyses and assessments are revised as appropriate	☒	☐
• Defined processes and specifications for the configuration and operation of the IT systems are adhered to and compliance is checked by the DPO (and IT audit)	☒	☐
• External inspections (audits) are carried out	☒	☐
• Certifications available (ISO 27001)	☒	☐

• IT security officer / information security officer (ISB) or a person responsible for information security with clearly defined allocation of competencies has been appointed	☒	☐
• Data Protection Officer was appointed	☒	☐
o DPO is consistently involved in security issues	☒	☐
o Audits are carried out regularly by the DPO in accordance with Art. 32 GDPR for the security of processing	☒	☐
o The DPO's cooperation with the IPM is supported by the company management	☒	☐
• Data protection impact assessment is carried out by the controller and the advice of the DPO is sought	☒	☐
• Technical and organizational measures are reviewed regularly and in the event of significant changes	☒	☐
• Appropriate safeguards for third country transfers are documented	☒	☐

2.4.3 Incident response management (incident response plans)

Incident response management is the documentation of all written instructions related to security incidents. It is used to detect security incidents and respond to them in an appropriate and predefined manner in order to limit damage.

2.4.3.1 Technical measures

	Yes	***No***
• Firewall deployment	☒	☐
• Use of antivirus software	☒	☐
• Use of spam filters	☒	☐
• Use of an online ticketing system	☒	☐
• Deployment of an intrusion detection system (IDS)	☒	☐
• Use of an Intrusion Prevention System (IPS)	☒	☐
• Use of a service hotline / helpdesk	☒	☐
• Blocking and reassignment of passwords after an incident is regulated	☒	☐

2.4.3.2 Organizational measures

	Yes	***No***
• Security and data incident detection and reporting process in place	☒	☐
• DPO and ISB are involved in security and data incidents	☒	☐
• Security and data incidents are documented	☒	☐
• Penetration tests are performed on a regular basis	☒	☐
• Data subjects can easily exercise their right of withdrawal	☒	☐

• Emergency concept is effectively implemented	☒	☐
• Emergency drills are conducted on a regular basis	☒	☐
• Emergency management is integrated into business processes	☒	☐

2.4.4 Data protection-friendly default settings (Art. 25 (2) GDPR)

Data protection-friendly default settings are technical and organizational measures designed to effectively implement the principles of data protection and to guarantee that legal requirements are met and data subjects' rights are protected.

	Yes	*No*
• Hardware and software is developed according to the privacy-by-design approach:	☒	☐
o Documentation of the development to enable audits	☒	☐
o Fine adjustment of user rights is enabled	☒	☐
o Encryption is enabled	☒	☐
o Software supports control measures by DPO / auditor (read access to data and logs)	☒	☐
o Data deletion / profile deletions are enabled and deletion routines are supported	☒	☐
o Data portability is enabled	☒	☐
o Checkboxes are disabled by default	☒	☐
o Contextual explanation of form fields, including free text fields	☒	☐
o Waiver of free text fields	☐	☒
• Use of hardware and software according to the privacy-by-default approach:	☒	☐
o Mandatory fields are limited to the required extent	☒	☐
o For self-entry in forms, fields are explained contextually, including free text fields	☒	☐
o Free text fields are not used	☐	☒
o User rights are limited to the necessary extent	☒	☐
o No automatic sharing of content with social media-enabled applications	☒	☐
o Maintainable information pages allow transparency	☒	☐

3 Do you have a question about data protection?

3.1 Ask atrify

At atrify, Ms. Rebecca Mannek, Legal Counsel, is available to answer your questions about data privacy as follows:

rmannek@atrify.com

For specific questions regarding this TOM, please contact Mr. Benjamin Herzog, Director Internal IT/ CISO, as follows:

bherzog@atrify.com

3.2 Ask the Data Protection Officer directly

atrify has appointed Dr. Herwig Pant as external Data Protection Officer. The Data Protection Officer is very happy to answer questions on data protection from clients, customers and employees of atrify.

Brands Consulting | Data Protection & Consulting
Dr. Herwig Pant
Auf dem Hahn 11
D-56412 Niedererbach

E-mail: atrify@brands-consulting.eu
Homepage: www.Brands-Consulting.eu

DocuSigned by:
Jochen Moll
BCB4B405D8784B6...

Jochen Moll, Managing Director