General Terms & Conditions

V4, effective from 15.10.2025

Table of contents

1 What is the Scope?

1.1 In Germany, Experian is represented by Experian GmbH, Baden-Baden, and infoscore Consumer Data GmbH, Baden-Baden (together referred to as “Experian”).

1.2 These General Terms and Conditions (the “Terms and Conditions”) govern the contractual relationship between Experian and each customer where the contract between Experian and the customer refers to these Terms and Conditions (each of Experian and the customer also a “Party” and together the “Parties”). Where the contract contains no express reference to these Terms and Conditions, only the provisions of the contract together with applicable regulatory provisions shall apply.

1.3 Experian may update these Terms and Conditions from time to time. The Terms and Conditions in force as at the date the contract is concluded shall apply. Any amendment of the Terms and Conditions by Experian to the detriment of the customer following an update shall only be effective by written agreement between the Parties.

1.4 If and to the extent of any conflict or inconsistency, the individually negotiated contract takes precedence over these Terms and Conditions.

2 What are the Primary Obligations?

2.1 Experian shall:

- **a.** provide the services in accordance with the provisions of the contract;
- **b.** exercise reasonable skill and care in providing the services (including in the collection and compilation of data on which the services are based or that are included in the services); and
- **c.** deploy suitably qualified personnel in providing the services.

2.2 The customer shall provide Experian with all information and support as agreed between the Parties in order for Experian to fulfil its obligations under the contract, and shall use reasonable endeavours to ensure that information provided to Experian is complete, accurate and in the agreed format.

2.3 Each Party shall:

- **a.** where a project timetable has been agreed, use all reasonable endeavours to perform its obligations in accordance with that timetable; and
- **b.** ensure that while its personnel are on the other Party’s premises they comply with that Party’s reasonable notified requirements relating to security and occupational health and safety.

2.4 Each Party warrants that:

- **a.** it has the authority to enter into the contract;

b. it has obtained and shall continue to obtain all licences, consents, approvals and agreements (to the extent required) necessary to perform its obligations under, and to grant rights to the other Party under, this agreement; and

c. the permitted use under this agreement of any information, data, software, documentation, scorecards and/or services that it provides to the other Party does not infringe third-party intellectual property rights in the Federal Republic of Germany.

2.5 Only warranties expressly set out in these Terms and Conditions are given by either Party in relation to the subject-matter of this agreement.

3 What is the Nature and Use of Data?

3.1 Experian's services are not intended to be used as the sole basis for business decisions and do not relieve the customer of its obligation to comply with applicable law.

3.2 Experian's services include models and techniques based on statistical analysis, probability and predictive behaviour. The customer acknowledges that it is prudent to use the services as one of several factors in its decision-making process and is responsible for determining those other factors. Where Experian, acting as controller, provides data to the customer, the customer acknowledges that such data is based on data supplied by third parties, the accuracy and/or completeness of which cannot be guaranteed by Experian.

3.3 The customer agrees that it will:

a. use the services and/or Experian Materials provided under this agreement only for the Permitted Purpose set out in the contract;

b. not sell, transfer, sub-licence, distribute, commercially exploit or otherwise make available to, or for the benefit of, any third party the services and/or Experian Materials provided under this agreement, except as expressly permitted in the contract;

c. not adapt, alter, modify, reverse engineer, decompile or otherwise interfere with (nor permit any third party to do so) the Experian Materials provided under this agreement, without Experian's prior written consent or other statutory permission; and

d. make only such copies of the Experian Materials as are reasonably required for use of the Experian Materials in accordance with the contract.

4 What are the Mutual Obligations?

4.1 Each Party must comply with all applicable laws that apply to it in connection with the provision or use (as the case may be) of the services.

4.2 To protect data and information security, both Parties must implement appropriate technical and organisational measures and maintain them in line with the state of the art, commensurate with the risks associated with processing. Without limitation, Experian is responsible for providing data and the interface for data access to the customer and for securing its systems and data against unauthorised third-party access; the customer is responsible for secure operation of its systems, data-processing programs and interfaces and for securing them against unauthorised third-party access.

4.3 To protect the integrity of data used in connection with the services, during the term the Parties shall:

a. comply with the data-security provisions, including those set out in Annex 1; and

b. not copy, interfere with and/or use in an unauthorised way any digital certificate, web certificate or other security device provided.

4.4 Before the customer is enabled for access to the systems and data, the customer must respond to information-security questions and provide appropriate evidence. After receipt, Experian will review the evidence and, following successful review, enable access within three business days.

4.5 Each Party permits the other Party, during the term, to verify compliance with the security requirements relating to the subject-matter of the service contract. Audits of internet-facing services, APIs and systems are permitted at any time subject to reasonable prior notice, during normal business hours and in coordination with the other Party. Audits of internal processes, in particular in the context of cyber and information security, are carried out by requesting appropriate evidence. Such evidence may be requested as needed but no more than once per year, subject to reasonable prior notice. Appropriate evidence includes, for example, certificates

(such as ISO/IEC 27001) or other suitable attestations (e.g. confirmations by the competent Information Security Officer (ISO) or Data Protection Officer (DPO)). Where appropriate evidence is provided, compliance is deemed demonstrated and no additional audit will take place. Should a Party wish to conduct an additional audit without cause within a contract year, it shall reimburse the audited Party for all reasonably and properly incurred costs arising from such additional audit. The Party conducting the audit must:

a. comply with the other Party's procedures for protecting confidential information about clients or customers of the other Party; and

b. take all reasonable steps to minimise disruption to the other Party's business during such audit.

4.6 User access devices or passwords (as applicable) are provided by Experian to enable the customer to access and use the services in accordance with this agreement. The customer shall ensure that user access devices or passwords are not copied and/or used in an unauthorised manner. It is the customer's responsibility to notify Experian of any unauthorised use and/or disclosure of a user access device or password so that Experian can block or disable it. The customer remains liable for any additional costs under the services arising in connection with use of a user access device or password until it has notified Experian.

5 Are the requirements regarding Consumer Protection?

5.1 The Parties shall cooperate and exchange information as required to ensure that both Parties meet their legal obligations and to help achieve positive outcomes for consumers.

5.2 The Parties further agree that, where statutory consumer-protection provisions apply in relation to the provision or use of the services, such provisions shall be complied with and the following additional provisions shall apply:

a. Where a consumer-protection duty applies to the customer's use of the services, the customer must determine its own method of distributing its products so that good customer outcomes are achieved based on a scientifically recognised mathematical-statistical procedure.

b. The customer must use the services in accordance with the Permitted Purpose and all other legal provisions relating to the use of, or restrictions on the use of, the services.

5.3 In addition, Experian reserves the right to assess and monitor whether the customer complies with the Permitted Purpose and all usage rights and restrictions and its obligations under this agreement. The customer shall provide Experian with all materials reasonably requested by Experian in order to carry out such assessment and review. The customer must also inform Experian of any breach of the Permitted Purpose and usage rights or restrictions. If, in Experian's reasonable opinion, the customer's use of the services does not comply with the Permitted Purpose or usage rights and restrictions, or if the customer breaches its obligations relating to any consumer-protection duty, the following procedure applies:

a. Experian shall notify the customer in text form specifying the breach and allow a period of 15 days to remedy the breach and ensure that the use of the services complies with the Permitted Purpose and the usage rights and restrictions.

b. If, in Experian's discretion, following expiry of the period in clause 5.3. the customer is still in breach, Experian reserves the right to suspend the customer's use of the services by written notice and grant a grace period of 28 days from receipt of the suspension notice within which the customer may remedy the breach.

c. If the non-compliance is remedied within the grace period referred to in clause 5.3.2, Experian shall lift the suspension. Otherwise, Experian reserves the right to terminate this agreement with immediate effect by written notice to the customer if either:

i. the non-compliance cannot be remedied; or

ii. the non-compliance can be remedied but the customer fails to do so within the above time limits.

5.4 The following further provisions apply:

a. The Parties undertake to act in good faith vis-à-vis end-customers;

b. The Parties must avoid foreseeable harm to end-customers;

c. The Parties must enable and support end-customers to pursue their financial objectives; and

d. If the customer ascertains that it or another undertaking in its distribution chain does not deliver outcomes for end-customers based on a scientifically recognised mathematical-statistical procedure, it must inform Experian without undue delay; likewise, if either Party ascertains or becomes aware that a communication by another undertaking in its distribution chain does not deliver outcomes based on a scientifically

recognised mathematical-statistical procedure for end-customers, it must inform the relevant undertaking in the distribution chain of the issue without undue delay.

5.5 If Experian makes findings as a result of (a) changes in applicable law (including a reasonable interpretation thereof), (b) changes in the provision of third-party data used in connection with the services, or (c) a security vulnerability which, in Experian's reasonable opinion, could harm consumers, Experian shall be entitled, following prior notice in text form to the customer, to take one of the following measures:

- **a.** suspend and/or amend the affected services to the extent required; or
- **b.** procure alternative data that are identical or comparable to the data used for the affected services; or
- **c.** terminate this agreement without liability in respect of the affected services.

6 Are there General Liability Provisions?

6.1 Experian shall be liable, regardless of the legal basis, only if the damage was caused by culpable breach of a material contractual obligation in a manner endangering achievement of the contract purpose, by injury to life, limb or health, by the German Product Liability Act (Produkthaftungsgesetz), or is due to gross negligence or wilful misconduct on the part of Experian. Experian shall be liable accordingly for its statutory representatives and vicarious agents.

6.2 In cases of slight negligence, liability is limited in amount to the typically foreseeable and avoidable damage.

6.3 If Experian is unable to perform due to force majeure or other unforeseeable, exceptional or unculpable circumstances, the period for performance is extended by the duration of the hindrance.

6.4 Data stored by Experian may be subject to change at any time, e.g. due to deletions or updates. The information provided to the customer therefore reflects the current status derived from the information available to Experian at the time.

6.5 It is solely the customer's responsibility to assess the impact of the information provided on its performance and business relationship with the data subject. In particular, Experian does not warrant fitness of the information for any specific purpose or result.

6.6 Individual caps on damages may be agreed between the Parties in the individual contract.

7 What are the warranty provisions?

7.1 The customer acknowledges that:

- **a.** in the case of data processing, the service only has statistical relevance for predicting a risk;
- **b.** where software uses statistical or empirical data and/or modelling techniques to predict a risk statistically, no specific result can be warranted or guaranteed by use of the service; and
- **c.** the outcome depends on the content and quality of data supplied to Experian.

7.2 The warranty is exclusively as set out in the agreed service levels and, where the requirements are met, the obligation to pay damages.

8 What are the regulations regarding Confidentiality?

8.1 Where confidential information is exchanged, the Party disclosing the information is the "Disclosing Party" and the Party receiving the information is the "Receiving Party".

8.2 The Receiving Party acknowledges that the confidential information disclosed to it was previously neither wholly nor partly known or accessible to it, is therefore of commercial value to the Disclosing Party, is kept secret by appropriate protective measures and that the Disclosing Party has a legitimate interest in its continued secrecy. Even where any confidential information does not meet the statutory requirements for a trade secret within the meaning of the German Trade Secrets Act (Gesetz zum Schutz von Geschäftsgeheimnissen – GeschGehG), such information shall nevertheless be subject to the obligations under this confidentiality clause to the extent it falls within a category of confidential information under this clause.

8.3 "Confidential information" comprises all information and data provided by the Disclosing Party to the Receiving Party, in particular:

- **a.** information covered by the Trade Secrets Act, i.e. trade secrets, analytical results, products, project work, analysis processes, know-how, designs, inventions, business relationships, business strategies, business plans, prices, financial planning and all information connected therewith;
- **b.** any documents, data and information of the Disclosing Party that are subject to technical and organisational secrecy measures, i.e. that are marked as confidential or would typically be regarded as confidential by a reasonable person in the context of initiating or conducting a business relationship;
- **c.** the precise content of this agreement; and
- **d.** any copies of information falling under the preceding bullets.

8.4 Information is not confidential if it:

- **a.** is or becomes generally known without breach of this agreement; or
- **b.** is lawfully disclosed to the Receiving Party by a third party without restrictions; or
- **c.** can be shown by the Receiving Party to have been lawfully in its possession prior to entry into force of this agreement or developed independently.

8.5 Each Party, as Receiving Party, undertakes to keep confidential and protect against disclosure, publication or dissemination the confidential information disclosed to it, except where the Party is subject to corresponding data-protection transparency obligations.

8.6 Each Party undertakes to apply at least the same degree of care and confidentiality as it applies (or ought to apply) to its own confidential information, i.e. to protect confidential information by appropriate confidentiality measures against unauthorised third-party access.

8.7 Each Party undertakes to disclose confidential information only for the above purpose and only to third parties of the Receiving Party to the extent necessary, provided that the Receiving Party ensures the third party complies with this agreement as if it were itself a Party.

8.8 Employees of the Parties, all undertakings affiliated with them within the meaning of sections 15 et seq. of the German Stock Corporation Act (AktG), all portfolio undertakings of the Parties and their professional advisers who are subject to confidentiality by agreement, professional rules or law and who are involved in the conclusion, review or performance of the contract on behalf of a Party are not regarded as third parties. This applies in particular to auditors, tax advisers, lawyers and management consultants.

8.9 Further, each Party, as Receiving Party, undertakes not to make reproductions or copies of confidential information unless strictly necessary. Any reproduction of confidential information, of whatever kind, may only be made for internal evaluation purposes and must be restricted to an absolute minimum.

8.10 Where disclosure of confidential information is required by law and/or government action, the Receiving Party obliged to disclose shall notify the Disclosing Party without undue delay so that the latter can obtain protective orders or take measures to safeguard confidentiality. The Receiving Party shall in addition use all reasonable endeavours to limit the scope of disclosure to a minimum and shall, where possible, support the Disclosing Party.

8.11 If the Receiving Party becomes aware of unauthorised reproduction, disclosure or use of confidential information of the Disclosing Party, it shall notify the Disclosing Party without undue delay and, at the Disclosing Party's request, take the necessary steps to prevent further unauthorised reproduction, disclosure or use.

8.12 The confidentiality obligation survives termination of this confidentiality undertaking and applies even if no business relationship is formed. After expiry of this period or achievement of the purpose set out in the preamble, and unless otherwise agreed or statutory retention duties apply, all confidential information held by the Receiving Party shall, without retaining copies, be returned to the Disclosing Party without request or, with prior written consent of Experian, be destroyed in full by the partner; where Experian is the Receiving Party, Experian's deletion concept applies without further duty to inform. Confidential information stored electronically or digitally must be destroyed by complete and irrevocable deletion of files or irreversible destruction of the data carrier so as to make any access to the confidential information impossible. The Parties shall delete the information upon completion of the project on the partner side and in accordance with Experian's deletion concept on the Experian side.

8.13 The Disclosing Party gives no warranty or liability for the accuracy or completeness of confidential information or for damage arising from its use. No licences to industrial property rights (including trade marks, designs, patents or utility models) and no rights of use in copyrighted materials, information or data or any other rights are granted by this agreement, by the provision of confidential information under this agreement or by other implied conduct. The Disclosing Party remains the owner of title, rights of use and rights of exploitation in the confidential information. Rights under the Trade Secrets Act remain unaffected. Any potential intellectual property rights in ICD materials, including ICD data, remain with ICD (or its licensors). “ICD Data” means data, personal data and/or databases and/or scores provided by ICD to the customer in connection with this agreement, but excluding customer data.

8.14 Experian designs and creates product presentations which constitute a protected work within the meaning of section 2(1) of the German Copyright Act (Urheberrechtsgesetz – UrhG). The Experian employee who creates the product presentation is the author of the protected work within the meaning of section 7 UrhG. Experian holds all necessary rights of use. In conducting product presentations, only Experian is entitled to make recordings of the presentations. Recordings are generally made using digital platforms such as Microsoft Teams as well as on site. Any breaks in the presentations are excluded from the recordings for privacy reasons. Before any recording by Experian, the consent of the participants will be obtained. After the recording has ended, it will be made available to the customer on Experian’s central data-exchange server.

8.15 The Receiving Party must refrain from exploiting or imitating, or having a third party exploit or imitate, the confidential information for any purpose beyond the purpose set out above; in particular, reverse engineering is prohibited, i.e. the Receiving Party must refrain from reconstructing/reverse-determining individual components of any service/product/information.

9 How is the Intellectual Property concluded?

9.1 All copyrights, database rights, domain names, patents, registered and unregistered design rights, registered and unregistered trade marks and all other industrial, commercial or intellectual property rights existing in any jurisdiction worldwide, and all rights to apply for any of the foregoing (together “Intellectual Property Rights”), in customer materials remain with the customer (or its licensors). “Customer Materials” means all items/documents provided to Experian by the customer in connection with the contract. To the extent any rights in Customer Materials or customer data pass to Experian by operation of law, Experian hereby assigns such rights to the customer.

9.2 All Intellectual Property Rights in Experian Materials remain with Experian (or its licensors). “Experian Materials” means the software and all materials, documentation, scorecards or other items/documents developed and/or licensed by Experian or any Experian company within the Experian group in connection with this contract. To the extent any rights in Experian Materials pass to the customer by operation of law, the customer hereby assigns such rights to Experian.

9.3 Experian grants the customer a non-exclusive, non-transferable licence to use the Experian Materials provided as part of the services for the Permitted Purpose. The licence granted under this clause is granted separately for each individual element of the Experian Materials and commences on the date the relevant element of the Experian Materials is first made available to the customer. The customer must not upload Experian Materials into third-party applications, including (without limitation) artificial-intelligence (“AI”) technologies, such as large language models and generative AI, as well as other AI technologies.

9.4 If at any time the foregoing conditions are not met, Experian shall be entitled to cease provision of all services with immediate effect.

9.5 Each Party:

- **a.** acknowledges and agrees that it has no claim to the Intellectual Property Rights of the other Party (or the other Party’s licensors) by virtue of the rights granted to it under this agreement, nor may it acquire or claim such rights through use of those Intellectual Property Rights;
- **b.** warrants that it will not at any time do or omit to do anything likely to prejudice the ownership of the other Party (or its licensors) in those Intellectual Property Rights; and
- **c.** undertakes not to remove, suppress or in any way alter proprietary notices, including trade marks or copyright notices, on or in the other Party’s materials and agrees to include such protected notices in all copies of those materials.

10 What applies in cases of force majeure?

10.1 Neither Party shall be liable for any delay or failure in performing its obligations under this agreement if such delay or failure results from force majeure.

10.2 If the force majeure persists for 28 days or more, the Party not relying on force majeure may notify the other Party that it terminates the contract with effect from a date specified in the notice, without penalty or other liability (save for the customer's obligation to pay accrued fees).

11 Are there any specific compliance requirements?

11.1 Each Party shall promptly report to the other Party:

- **a.** any request or demand for an undue financial or other advantage made or received in connection with the contract;
- **b.** any form of slavery or human trafficking in a supply chain connected with the contract;
- **c.** any request or demand from a third party to facilitate/enable tax evasion in connection with performance of this contract.

11.2 Each Party may expect the other Party to conduct its business with integrity, in particular by complying with all applicable laws (for example, in relation to human rights including the ILO core labour standards, anti-corruption, data protection, competition and antitrust) and to ensure that such requirements are likewise met by its own business partners; both Parties shall promote such requirements and act honestly, responsibly and fairly. Each side may, where necessary, request evidence of control measures from the other Party.

11.3 The Parties further undertake to use natural resources efficiently and to take measures to reduce waste, emissions and energy consumption.

11.4 The Parties must inform and oblige their employees, insofar as they are involved in cooperation with the other Party, to comply with the relevant provisions of data-protection law.

11.5 The customer must not copy, interfere with and/or use in an unauthorised way any identification codes, user names, passwords, digital certificates, web certificates or other security device ("User Access Device") provided by Experian and used by the customer to access the services.

11.6 The customer must comply with Experian's reasonable instructions and security policies regarding access to Experian systems, including those set out in the security guidelines (https://ssp.uk.experian.com/securecontrol/securityGuidelines.html).

11.7 The customer must inform Experian of any unauthorised use and/or disclosure of a User Access Device so that Experian can suspend or deactivate that access. The customer is liable for all service fees incurred in connection with use of a User Access Device until it has notified Experian.

11.8 The Parties agree that each Party processes customer or supplier data for the purposes of providing the services contemplated by this agreement within the agreed purposes.

12 What applies with regard to system availability or processing times?

12.1 System availability is at least 98%, subject to planned maintenance. Planned maintenance takes place on the third weekends in February, May, August and October, commencing at 01:00 on Sunday. Maintenance is generally completed by 05:00. With general operating hours of 7x24 hours a week, the services are unavailable once per calendar month between 00:00 and 08:00 for a maximum of two hours.

12.2 Where the manufacturer urgently recommends "security patches", deployment takes place within 24 hours between 02:00 and 06:00. Planned downtimes are generally announced with at least 24 hours' notice. Maintenance weekends are announced 10 working days in advance. Announcements are made by email.

12.3 The response time (time between receipt of the request by Experian and dispatch of the result by Experian, i.e. excluding transmission speed) for online credit enquiries is generally under two seconds. Any processing times for related ancillary services are additional.

12.4 For credit enquiries submitted by file transfer (batch processing), the results for volumes of up to 5,000 data records are generally returned within two hours.

13 What are the technical requirements?

13.1 Experian strives to maintain system availability and performance at the highest possible level. The production system is therefore not generally available for testing. Any tests intended by the customer must in any case be agreed with Experian in advance. In particular, the customer undertakes to agree any planned load/performance tests with IT Support at least seven days in advance. In the case of unannounced load/performance tests that impair or jeopardise system availability and performance, Experian reserves the right to suspend access temporarily. For the same reasons, foreseeable load spikes involving an increase of more than 50% over the average request volume of the last three months must be communicated to IT Support at least 14 days in advance.

13.2 Experian provides an IT Support function that is available to the customer during the specified service hours via the specified contact details. IT Support is the single point of contact (SPOC) for the customer. Service hours are Monday to Friday 08:00–18:00 (excluding public holidays in Baden-Württemberg).

14 What applies in the event of third-party infringement of licensed materials?

14.1 The customer must inform Experian without undue delay if it becomes aware of any infringement of Experian's rights in the licensed materials or of circumstances that may lead to an actual or future infringement.

14.2 In the event of a threatened infringement of intellectual property rights or other rights in connection with use of the software, the Parties shall notify each other in writing without undue delay, in particular where claims are asserted against them or where there are indications thereof. No settlement may be concluded, admission made or other concession given by either Party in relation to any asserted claim without the written consent of the other. If a claim or action for infringement is brought or, in Experian's reasonable assessment, threatens to be brought, Experian may, at its own cost, take measures to avoid the infringement or alleged infringement, in particular by non-infringing modification or replacement of a service or by procuring a licence permitting the use.

14.3 Experian is entitled to take legal action in respect of infringements of its rights in licensed materials.

15 What are the final provisions?

15.1 The Parties are not entitled to assign rights and obligations under the contractual relationship to third parties or transfer the contract as a whole unless the other Party has given prior written consent to the assignment. The right to withhold payments or to set off claims is excluded unless Experian has given prior written consent to the set-off.

15.2 Amendments to this agreement are only effective if recorded in writing and signed by the Parties (signature may be by electronic signature). However, amendments to the timetable made in accordance with an agreed change-control procedure are effective.

15.3 Failure or delay by Experian in exercising any right, power or remedy does not constitute a waiver thereof, nor does any partial exercise preclude any further exercise of the same or any other right, power or remedy.

15.4 The contract together with these Terms and Conditions contains the entire agreement between the Parties regarding its subject-matter and supersedes all prior (oral or written) agreements between the Parties regarding the same subject-matter. Each Party acknowledges that, in entering into the contract, it does not rely on any negligent warranty or representation not set out in this agreement and has no claim in that respect.

15.5 Nothing in the contract or these Terms and Conditions is intended to, or shall be construed to:

- **a.** constitute any partnership or joint venture (for example a Gesellschaft bürgerlichen Rechts (GbR) under sections 705 et seq. German Civil Code (BGB)) of any kind between the customer and Experian;
- **b.** authorise either Party to act as agent for the other; or
- **c.** authorise either Party to act in the name of or on behalf of the other or to bind the other in any way.

15.6 If any provision of the foregoing is or becomes wholly or partly invalid, the validity of the remaining provisions shall not be affected. Any invalid provision shall be replaced by a legally permissible provision that comes as close as possible to the original economic intent of the Parties.

15.7 If statutory provisions or requirements of competent authorities render further cooperation legally impossible or no longer economically viable, Experian reserves the right to modify the contractual services or to terminate the contract for cause. Where possible, Experian shall give reasonable advance notice of any modification or termination. The customer shall have no claims against Experian arising from any such modification or termination.

15.8 The contract is governed by the law of the Federal Republic of Germany, excluding conflict-of-laws rules. The application of the UN Convention on Contracts for the International Sale of Goods (CISG) is excluded.

15.9 These Terms and Conditions are also provided in English. In case of doubt or translation errors, the German text prevails.

16 Annex 1: Experian Security Requirements

16.1 The security requirements in this document represent the minimum security requirements acceptable to Experian and are intended to ensure that the Parties have appropriate controls in place to protect information and systems, including all information that they receive, process, transmit, transfer, store, provide and/or otherwise access on behalf of Experian.

16.2 The definitions used in this document have the following meanings:

a. "Information" means sensitive information of either Party, such as, for example, data, databases, application software, software documentation, supporting process documents, documentation of operational processes and procedures, test plans, test cases, test scenarios, cyber incident reports, consumer information, financial data, employee data and information on potential acquisitions, as well as other information of a similar nature or as mutually agreed in writing, the disclosure, alteration or destruction of which would seriously damage Experian's reputation or valuation and/or put Experian at a competitive disadvantage.

b. "Resource" means any third-party-managed information technologies, systems, devices and applications that store, process, transmit, transfer or access Experian information or otherwise relate to the provision of contractually agreed services for Experian.

16.3 The Parties must have, maintain and disseminate information-security strategies, standards and procedures relevant to their operating environment and ensure they are reviewed at planned intervals or upon significant changes to ensure their continued suitability, adequacy and effectiveness.

16.4 The Parties shall require all employees to complete at least annual information-security and awareness training and shall document evidence of completion for all employees.

16.5 The Parties manage personnel security risk by vetting individuals, before granting access privileges, to a level appropriate to their intended role.

16.6 The Parties proactively manage individual, group, system and application login accounts and ensure that the creation of all accounts and the assignment of access rights is governed by formal registration. Privileged accounts must be restricted to specific persons or roles. All accounts, privileges and access rights must be reviewed, validated and, where necessary, changed on a regular basis.

16.7 The Parties must set requirements for complexity, length and lifetime to ensure strong criteria for password-based authentication and must implement such requirements consistently across all systems and applications. Multi-factor authentication (MFA) shall be used for access to networks, resources and privileged access scenarios, based on organisationally defined requirements.

16.8 Technical vulnerabilities must be consistently identified, prioritised, tracked and remediated across all resources, systems, infrastructures and both hosted and developed applications. Proactive software patching must be performed on a defined schedule.

16.9 All internet-facing resources involved in the delivery of services for Experian must be subjected to at least annual penetration or web-application security testing.

16.10 Endpoints must be managed so as to ensure a consistent security configuration and to allow installation of approved software only.

16.11 Anti-malware technologies must be deployed to detect and remove malicious code on endpoints.

16.12 Cryptographic measures must be used to protect the confidentiality of information at rest and in transit to prevent unauthorised disclosure.

16.13 The Parties shall design and implement firewall and router configurations between untrusted and trusted networks according to the principle of least privilege and review them at least annually. All remote access to resources and information is via managed network access-control points.

16.14 Logging and monitoring requirements must be defined, with the monitoring of resources prioritised according to their criticality and the sensitivity of the information they store and process.

16.15 Event logs and alerts must be continuously reviewed and inappropriate or unusual activities that have actual or potential impact on a security incident must be reported in line with the defined deadlines and procedures.

16.16 Procedures must be defined, and regularly tested, to facilitate response to potential or actual security incidents and personal-data breaches in order to ensure continuity of operations.

16.17 Changes to systems, applications and infrastructures must be authorised, planned, approved, tested and evaluated in accordance with a defined process or procedure. Operational authorities for changes must be restricted to authorised personnel.

16.18 The Parties are subject to remote and/or on-site assessment of their information-security controls and compliance with these security requirements.

16.19 The Parties must not send “bulk emails” to the other Party’s employees without the other Party’s prior approval. Approval must be obtained via the relevant Key Account Manager before the process is initiated.

16.20 To ensure appropriate protection of user accounts, the Parties undertake, when setting up user accounts, to comply with a minimum password length of twelve (12) characters. Passwords must combine upper- and lower-case letters, numbers and special characters and must not contain easily guessable terms or simple character sequences. This measure is intended to increase password complexity and defend against automated attacks.

16.21 The Parties undertake to change passwords at the latest every six (6) months. This replaces earlier, shorter change intervals and follows current security standards that prioritise the uniqueness and complexity of passwords over frequent changes.

16.22 Use of passwords that appear in standard dictionaries or have already been compromised in publicly known data breaches is prohibited. Both Parties may implement technical measures that automatically detect and block such passwords. The Parties are obliged to use only secure and uncompromised passwords.