Auftragsdatenverarbeitungsvertrag gemäß Art 28 DSGVO

zwischen

Glühende Kante e.V., vertreten durch

Walter Call, Mühlental 18, 52066 Aachen &

Lukas Hirschwald, Gartenstr. 36, 52064 Aachen

KundenNr/ID: 9010

(im Folgenden: Auftraggeber)

und

Netxp GmbH
Öttinger Straße 11
84307 Eggenfelden

(im Folgenden: Auftragnehmer)

Präambel

Die Parteien haben einen Vertrag über die Pflege, Administrierung und Bereitstellung der in der Anlage 1 zum vorliegenden Vertrag beschriebenen Software-Anwendung geschlossen, (Im folgenden „Hauptvertrag“). In diesem Zusammenhang ist der Auftragnehmer verpflichtet, die Anforderungen der Art 25 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) und 32 (Sicherheit der Verarbeitung) DSGVO zu erfüllen. Ebenso ist der Auftragnehmer verpflichtet der Auftraggeberin die im Hauptvertrag beschriebene Softwareanwendung zur Verfügung zu stellen, zu administrieren und zu pflegen, bzw. weiter zu entwickeln.

In Rahmen der Administrierung, Pflege bzw. Weiterentwicklung, der in der Anlage 1 beschriebenen Software-Anwendung, hat der Auftragnehmer Zugriff auf die in der Anlage 2 des vorliegenden Vertrages dargelegten personenbezogenen Attribute.

Dieser Vertrag konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der in der Anlage 1 des vorliegenden Vertrages in ihren Einzelheiten beschriebenen Auftragsdatenverarbeitungstätigkeiten ergeben. Sie findet Anwendung auf alle Tätigkeiten, bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

Diese Vereinbarung wird durch ihre Unterzeichnung gültig und gilt bis zu ihrer Kündigung.

§ 1 Definitionen:

(1) Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse

einer bestimmten oder bestimmbaren natürlichen Person.

(2) Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Speicherung, Veränderung, Übermittlung, Sperrung oder Löschung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers.

(3) Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Sie können durch Einzelweisungen ergänzt werden.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich („Verantwortlicher“ im Sinne des Art. 4 (7) EU-DSGVO). Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrnehmung seiner Verantwortlichkeit.

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch nach der Laufzeit des Vertrages und nach Beendigung des Vertrages die Herausgabe oder Löschung der Daten verlangen.

(3) Die Inhalte dieses Vertrages gilt entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen.

(2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

(3) Der Auftragnehmer sichert in seinem Verantwortungsbereich die Umsetzung und Einhaltung der vereinbarten allgemeinen und technischen und organisatorischen Maßnahmen entsprechend Art. 25 EU-DSGVO zu. Insbesondere wird der Auftragnehmer seine innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie wird technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten des Auftraggebers vor Missbrauch und Verlust treffen, die den Forderungen der EU-DSGVO entsprechen. Dies beinhaltet insbesondere

- Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle),

- zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

- dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

- dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

- dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

- dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

- dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

- dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle).

(4) Der Auftragnehmer stellt dem Auftraggeber ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept (Security-Policy bzw. Auflistung der beim Auftragnehmer eingeführten technischen und organisatorischen Maßnahmen zur Realisierung eines hinreichenden Datensicherheitsniveaus) zur Verfügung. Dieses Datensicherheitskonzept liegt dem vorliegenden Vertrag als Anlage 3 bei.

(5) Der Auftragnehmer stellt dem Auftraggeber die für das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO notwendigen Angaben zur Verfügung.

(6) Der Auftragnehmer stellt sicher, dass die mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter gemäß Art. 28 (3) b. zur Vertraulichkeit (Datengeheimnis) verpflichtet und in die Schutzbestimmungen der EU-DSGVO eingewiesen worden sind.

(7) Als Datenschutzbeauftragte(r) ist beim Auftragnehmer Herr [Martin Ammer Telefon: 08721506480 Email: martin.ammer@netxp.de] bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

(8) Der Auftragnehmer unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufes, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten bei der Verarbeitung der Daten des Auftraggebers.

(8) Überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit seine Daten und Unterlagen betroffen sind. Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial übernimmt der Auftragnehmer auf Grund einer Einzelbeauftragung durch den Auftraggeber. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(10) Der Auftragnehmer sichert zu, dass die im Zusammenhang mit der Vertragserfüllung gespeicherten Daten nur im Gültigkeitsbereich der EU-DSGVO gespeichert, verarbeitet und genutzt werden.

(11) Der Auftragnehmer versichert, dass die personenbezogenen Daten nicht für eigene Zwecke genutzt werden und eine Datenübermittlung nur auf Grundlage dieser Vertragsanlage erfolgt.

(12) Der Auftragnehmer unterstützt den verantwortlichen Auftraggeber bei der Einhaltung der in den art. 32 bis 36 EU-DSGVO genannten Pflichten.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber und der Auftragnehmer sind bzgl. der zu verarbeitenden Daten für die Einhaltung der jeweils für sie einschlägigen Datenschutzgesetze verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Die Pflicht zur Führung des Verzeichnisses der Verarbeitungstätigkeiten liegt beim Auftraggeber. Der Auftragnehmer unterstützt ihn dabei gemäß Art. 30 (2) EU-DSGVO.

(4) Über die Herausgabe oder Löschung der Daten nach Vertragsende (§ 2 (2)) muss der Auftraggeber innerhalb einer von dem Auftragnehmer gesetzten Frist entscheiden.

(5) Entstehen nach Vertragsbeendigung zusätzliche Kosten durch die Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber.

§ 5 Anfragen Betroffener an den Auftraggeber

Ist der Auftraggeber aufgrund Kapitel III EU-DSGVO gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber gemäß Art 28 (3) e) EU-DSGVO dabei unterstützen, diese Informationen bereit zu stellen.

§ 6 Kontrollrecht

Der Auftraggeber kann sich gemäß Art 28 (3) h) nach rechtzeitiger Anmeldung zu Prüfzwecken in den Betriebsstätten zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs von der Angemessenheit der Maßnahmen zur Einhaltung der technischen und organisatorischen Erfordernisse überzeugen.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer umfassenden Auftragskontrolle erforderlich sind.

§ 7 Subunternehmer

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer zur Erfüllung seiner vertraglich vereinbarten Leistungen verbundene Unternehmen des Auftragnehmers zur Leistungserfüllung heranzieht bzw. Unternehmen mit Leistungen unterbeauftragt.

Eine Auflistung der eingeschalteten Subunternehmer mit den jeweils übertragenen Aufgabenfeldern findet sich in der Anlage 4 des vorliegenden Vertrages.

(2) Sollen weitere/andere Dienstleister, unterbeauftragt werden, so muss diese in einer Mitteilung, eine angemessene Zeit vorab schriftlich, elektronisch (z.b. Email oder Meldung bei Start der Software) oder in Textform informiert werden. In diesem Fall ist die Anlage 4 des vorliegenden Vertrages anzupassen.

(4) Werden Subunternehmer durch den Auftragnehmer eingeschaltet, so werden die vertraglichen Vereinbarungen so gestaltet, dass sie den Anforderungen zu Vertraulichkeit, Datenschutz und Datensicherheit zwischen den Vertragspartnern dieses Vertrages entsprechen. Dem Auftraggeber sind Kontroll- und Überprüfungsrechte entsprechend Art 28 (3) h) EU-DSGVO einzuräumen. Ebenso ist der Auftraggeber berechtigt, auf schriftliche Anforderung des Auftragnehmers Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen.

§ 8 Sonstiges, Allgemeines

(1) Sollten die Daten des Auftraggebers bei dem Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es gilt deutsches Recht. Ist der Auftraggeber Kaufmann oder eine juristische Person des öffentlichen Rechts oder verlegt er seinen Wohnsitz nach dem Vertragsschluss ins Ausland, ist für alle Streitigkeiten das für den Auftragnehmer zuständige Gericht ausschließlich zuständig.

§ 9 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Glühende Kante e.V.
Hochschulsportzentrum Aachen
Mies-van-der-Rohe-Straße
52074 Aachen

Aachen, 23.01.2022

(Ort, Datum)

(Unterschrift [Auftraggeber])

Netxp GmbH
Öttinger Straße 11
84307 Eggenfelden
Telefon: 08721/50 64 8-0
Telefax: 08721/50 64 8-50
eMail: info@netxp.de
Internet: www.netxp.de

Eggenfelden, 24.01.2019

(Ort, Datum)

(Unterschrift Auftragnehmer)

Anlage 1 Netxp:Verein

Mit der Online-Vereinsverwaltung arbeitet der Auftraggeber in seinem Verein mit beliebig vielen Benutzern und nur EINEM Datenbestand. Diese Daten werden zentral auf gesicherten Servern des Auftragnehmers gespeichert. Der Auftraggeber kann seinen Benutzern verschiedene Rechte zuweisen.

Der Auftraggeber wird es durch Einsatz der Software ermöglicht sämtliche Finanzangelegenheiten Ihres Vereins über Netxp:Verein abzuwickeln. So können Sie das integrierte HBCI-SEPA Online-Banking nutzen um sämtliche Bankgeschäfte online durchzuführen. Mit der integrierten Vereinsbuchhaltung haben Sie die Finanzen Ihres Vereins im Griff und das Erstellen von Kassenbüchern und Einnahmen- Ausgabenrechnungen erledigen Sie in einem Bruchteil der normalen Zeit.

Um eine möglichst große und gute Außenwirkung zu erzielen ist es nötig, mit Vereinsmitgliedern in Kontakt zu bleiben. Mit Netxp:Verein ist es möglich Serienbriefe, SMS oder Serien-Emails zu versenden

Anlage 2 Netxp:Verein

Mit Netxp:Verein können folgende Personengruppen gespeichert werden:

- Mitglieder aktiv/ Passiv Ausgetreten
- Interessenten
- Lieferanten
- Kunden

Folgende Daten können zu den jeweiligen Personengruppen gespeichert werden

- Anrede, Titel, Vorname, Nachname
- Anschrift, Telefonnummer, Handynummer, Emailadresse
- Bankverbindung,
- Vereinsmitgliedschaft
- Eigene zu definierende Felder
  - ☒ Geburtsdatum
  - ○ _____
  - ○ _____
  - ○ _____
  - ○ _____
  - ○ weitere auf separatem Blatt

Anhang3 Technische und Organisatorische Maßnahmen gemäß Art 32 EU-DSGVO bzw. der Anlage zu § 9 BDSG

Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- verschlossene Türen und Fenster bei Abwesenheit
- Festlegung von zusätzlich schwer gesicherten Sicherheitsbereichen
- Zutrittskontrollsystem durch kontrollierte Schlüsselvergabe bzw. Schließsysteme
- Protokollierung der Zu- und Abgänge in Sicherheitsbereichen
- Zutrittsregelungen für nicht autorisierte Personen. Zutritts-, Zugangs- und
- Zugriffsberechtigungen werden nur von autorisierten Personen ausgeübt.
- Überwachungseinrichtung (Alarmanlage, Kameraüberwachung)

Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Identifizierung und Authentifizierung einschließlich Verfahrensregelungen zur Kennwortvergabe
- Einsatz komplexer Kennwörter mit regelmäßiger Änderung und Historie oder höherwertige Maßnahmen (z.B.: Biometrisch-, 2-Faktor Authentifizierung)
- Protokollierung durch Logbuch
- Einsatz mehrerer unterschiedlicher Firewalls
- Verschlüsselungsverfahren bei Datenverarbeitung

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Berechtigungskonzept mit differenzierten Berechtigungen
- Identifizierung und Authentifizierung
- Verschlüsselungsverfahren entsprechend dem Stand der Technik

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Verschlüsselung von Daten bei der elektronischen Übertragung entsprechend dem Stand der Technik
- Festlegung und Beschränkung des Empfängerkreises von Daten
- Regelungen für den Transport von Datenträgern

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierungs- und Protokollauswertungssystem bezüglich sämtlicher Systemaktivitäten durch Logbuch
- datenschutzgerechte Aufbewahrung der Protokolle durch den Auftragnehmer für einen definierten Zeitraum

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- schriftliche Festlegung der Weisungen
- regelmäßige interne Kontrolle und Dokumentation des Auftragnehmers, dass Weisungen und Regelungen zur Auftragsdurchführung beachtet werden

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Backup-Verfahren mit regelmäßiger Speicherung (on-site/off-site)
- Verwendung von gespiegelten Festplatten
- Unterbrechungsfreie Stromversorgung durch Stromaggregat und USV
- Brandmelder und Überwachungssystem

Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- interne Mandantenfähigkeit
- Trennung von Test und Produktion

Anlage 4 Subunternehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung
Microsoft	Westeuropa/ Deutschland	Hosting, Backup Anbindung
1&1 Internet SE	Elgendorfer Str. 57 56410 Montabaur Deutschland	Hosting, Backup Anbindung