Verzeichnis von Verarbeitungstätigkeiten gem. Art 30 Abs. 1 DS-GVO

Erfassung einer Verarbeitungstätigkeit

Angaben zur Verarbeitung	
Bezeichnung des Verfahrens/ Verarbeitungstätigkeit: Führen eines Mitgliederverzeichnisses der Mitglieder der Kulturwerkstatt Paderborn	
	Bitte zutreffendes ankreuzen: ☐ Änderung bestehender Verarbeitung ☒ neue Verarbeitung ☐ Abmeldung bestehender Verarbeitung ☐ Anpassung DS-GVO
Angaben zum Verantwortlichen *(Name und Kontaktdaten natürliche Person/ juristische Person/ Behörde/ Einrichtung etc.)*	
Stadt Paderborn Der Bürgermeister Am Abdinghof 11 33098 Paderborn Tel.: 05251 88 - 0 Fax.: 05251 88 – 2000 E-Mail: info@paderborn.de	
Angaben zur Vertretung *(nur bei Niederlassung in Drittstaaten/ Anbieter in Drittstaaten, Name und Kontaktdaten natürliche Person/ juristische Person/ Behörde/ Einrichtung etc.)*	
Angaben zum/zur Datenschutzbeauftragten *(Name und Kontaktdaten)*	
Datenschutzbeauftragte der Stadt Paderborn beim Kommunalen Rechenzentrum Minden-Ravensberg/Lippe Bismarckstr. 23 32657 Lemgo Tel.: 05261 252 – 0 Fax.: 05261 252 - 200 E-Mail: datenschutzbeauftragte@krz.de.	
Verantwortliche Fachabteilung *(Name und Kontaktdaten) (Art. 30 Abs. 1 S. 2 lit a)*	
Kulturwerkstatt Paderborn Bahnhofstr. 67 33102 Paderborn 05251-31785	

kulturwerkstatt@paderborn.de

1. Allgemeine Angaben

Datum der Einführung:
23.07.2018
Datum der letzten Änderung:

2. Zwecke der Verarbeitung

Zweckbestimmung

Führen eines Mitgliederverzeichnisses der Mitglieder der Kulturwerkstatt Paderborn

Rechtsgrundlage (zutreffende bitte ankreuzen und erläutern sowie ggf. nach Art der Datenverarbeitung unterscheiden)

☐ Spezialgesetzliche Regelung außerhalb der DS-GVO (Bitte benennen: Vorschrift, Paragraph, Absatz, Satz)

☒ Einwilligung des Betroffenen (Art. 6 Abs. 1 a) DS-GVO)

☐ Kollektivvereinbarungen (z.B. Dienst-/Betriebsvereinbarung, Tarifvertrag): (Bitte benennen: genaue Bezeichnung, Paragraph, ggfs. Absatz)

☐ Begründung, Durchführung oder die Beendigung eines Beschäftigungsverhältnisses (national geregelt in BDSG oder LDSG):

☐ Vertrag oder Vertragsanbahnung mit dem Betroffenen ((Art. 6 Abs. 1 b) DS-GVO):

☐ Interessenabwägung ((Art. 6 Abs. 1 f) DS-GVO): (Bitte benennen Sie die vorrangigen Interessen)

☐ Sonstiges

3. Kategorien der betroffenen Personen / Kreis der Betroffenen

(Art.30 Abs. 1 S. 2 lit. c)

Bezeichnung der Daten
Mitglied der Vereinigung Kulturwerkstatt
Vorstand der Vereinigung Kulturwerkstatt

4 Kategorien der personenbezogenen Daten

(Art.30 Abs. 1 S. 2 lit. c)

Lfd. Nr.	Bezeichnung der Daten	Besondere Kategorien personenbezogener Daten (Art. 9)
1	Name, Vorname	☐
2	Adresse	☐
3	Telefon, Handy, Mail	☐
4	Art der kreativen/sozialenTätigkeit in der Kulturwerkstatt	☐
5	ggf. Vereinszugehörigkeit	☐
6		☐

5. Kategorien der Empfänger der Daten

(Art.30 Abs. 1 S. 2 lit. d)

Lfd. Nr. aus Ziffer 4	Empfänger	intern	extern	Drittland
1-5	Dez III, Ämter 01, 13, 14, 20, 41, 44, 47	☒	☐	☐
1-5	Medienhaus Paderborn, Internet/Facebook	☐	☒	☒
1-5	Vorstand: lokale Presse	☐	☒	☒

6. Übermittlung von pers.-bez. Daten an ein Drittland oder an eine internationale Organisation

☐ **Datenübermittlung findet nicht statt und ist auch nicht geplant.**

Lfd. Nr. aus Ziffer 4	Drittland oder internationale Organisation	Geeignete Garantien im Falle einer Übermittlung gem. Art. 49 Abs. 1 Unterabsatz 2 DS-GVO
1-5	Internet/Facebook	

7. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien

(Art.30 Abs. 1 S. 2 lit. d)

Lfd. Nr. aus Ziffer 4	Löschfrist/en (Aufbewahrungsfristen oder sonstige einschlägige Löschungsfristen)
1-5	Bis auf Widerruf, Tod oder Erlöschen der Mitgliedschaft; danach internes Archiv

8. Technische und organisatorische Maßnahmen

(Art. 32 Abs. 1 DS-GVO)

Maßnahmen zur Pseudonymisierung, z. B.

- Festlegung der durch Pseudonymisierung zu ersetzenden identifizierenden Daten
- Definition der Pseudonymisierungsregel, ggf. anknüpfend an Personal-, Kunden- oder Patienten-Kennziffern
- Autorisierung: Festlegung der Personen, die zur Verwaltung der Pseudonymisierungsverfahren, zur Durchführung der Pseudonymisierung und ggf. der Depseudonymisierung berechtigt sind
- Festlegung der zulässigen Anlässe für Pseudonymisierungs- und Depseudonymisierungsvorgänge
- zufällige Erzeugung der Zuordnungstabellen oder der in eine algorithmische Pseudonymisierung eingehenden geheimen Parameter
- Schutz der Zuordnungstabellen bzw. geheimen Parameter sowohl gegen unautorisierten Zugriff als auch gegen unautorisierte Nutzung
- Trennung der zu pseudonymisierenden Daten in die zu ersetzenden identifizierenden und die weiteren Angaben

Welche Maßnahmen wurden getroffen (Bitte beschreiben):

Verschlüsselung, z. B.

- zufällige Erzeugung der Schlüssel
- Autorisierung von Personen zur Verwaltung und zur Nutzung von Schlüsseln bzw. ihre Zuweisung zu Geräten, in denen sie eingesetzt werden
- zuverlässige Schlüsselverteilung, Verknüpfung von Schlüsseln mit Identitäten von natürlichen Personen oder informationstechnischen Geräten, ggf. Einbringen in speziell gesicherte Speichermedien (z. B. Chipkarten)
- Schutz der Schlüssel vor nicht autorisiertem Zugriff oder Nutzung
- regelmäßiger oder situationsbezogener Schlüsselwechsel, ggf. eine Schlüsselarchivierung, stets sorgfältige Schlüssellöschung nach Ablauf des Lebenszyklusses
- Verwaltung des Lebenszyklus der Schlüssel von Erzeugung und Verteilung über Nutzung bis zu ihrer Archivierung und Löschung

Welche Maßnahmen wurden getroffen (Bitte beschreiben):

Vertraulichkeit, z. B.

- Formulierung von verbindlichen Sicherheitsleitlinien
- Definition der Verantwortlichkeiten für das Informationssicherheitsmanagement
- Inventarisierung der zu verarbeitenden personenbezogenen Daten
- Inventarisierung der Informationstechnik
- Erarbeitung eines Sicherheitskonzepts, ggf. unter Durchführung einer Risikoanalyse
- Personalsicherheit: Überprüfung und Verpflichtung des Personals, Sensibilisierung und Training, Aufgabentrennung
- Spezifikation der Sicherheitsanforderungen an Informationssysteme und deren Konfiguration, Prüfung ihrer Einhaltung
- Schutz vor unberechtigtem physischem Zugang, einschließlich Schutz von Mobilgeräten

- Erarbeitung eines Rollen- und Rechtekonzepts
- o Maßnahmen zur Autorisierung von Personen für den Zugriff auf personenbezogene Daten und die Steuerung der Verarbeitung
- o Zugriffskontrolle und sicherer Umgang mit Speichermedien, einschließlich der Maßnahmen zur zuverlässigen Authentisierung von Personen gegenüber der Informationstechnik, zur Sicherung der Revisionsfähigkeit der Eingabe und der Änderung von personen-bezogenen Daten sowie ggf. der Nutzung und des Zugriffs auf diese und zur Revision dieser Prozesse
- o Maßnahmen der Betriebssicherheit, insbesondere zur Spezifikation der Bedienabläufe, zur Änderungssteuerung, zum Schutz vor Malware, zum Umgang mit technischen Schwachstellen, zur kontrollierten Installation und Konfiguration neuer Software, sowie zur Ereignisüberwachung und -protokollierung, einschließlich der regelmäßigen und anlassbezogenen Auswertung dieser Protokolle

Welche Maßnahmen wurden getroffen (Bitte beschreiben):

Personalschulung – Sichtbarkeit nur für MitarbeiterInnen der Kulturwerkstatt. Vertraulichkeitsschulung intern.

Datenzugriff nicht von außerhalb – geschütztes Netzwerk der Stadt Paderborn.

Integrität, z. B.

- Maßnahmen, die (berechtigte oder unberechtigte) Veränderung gespeicherter oder übertragener Daten nachträglich feststellbar machen (z. B. Signaturverfahren, Hashverfahren)
- Maßnahmen zur Kommunikationssicherheit: Netzwerksicherheitsmanagement, insbesondere zur Kontrolle und Einschränkung des Datenverkehrs (Firewalls, Application Layer Gateways), Einrichtung von Sicherheitszonen, Authentisierung von Geräten gegeneinander
- sichere Gestaltung von Informationsübertragungen, einschließlich des Abschlusses von Vereinbarungen mit regelmäßigen Übermittlern und Empfängern personenbezogener Daten und der Authentisierung der Kommunikationspartner
- Sicherung und Überprüfung der Authentizität der übermittelten Daten
- sichere Einbeziehung von externen Diensten
- Management von Informationssicherheitsvorfällen
- Aufrechterhaltung der Informationssicherheit bei ungeplanten Systemzuständen
- Durchführung von internen oder externen Sicherheitsaudits
- logische oder physikalische Trennung der Datenverarbeitung z. B. nach verantwortlichen Stellen, den verfolgten Verarbeitungszwecken und nach Gruppen betroffener Personen
- sicheres, rückstandsfreies Löschen von Daten bzw. Vernichten von Datenträgern nach Ablauf der Aufbewahrungsfristen, Festlegungen zu Löschverfahren und zur Beauftragung von Dienstleistern

Welche Maßnahmen wurden getroffen (Bitte beschreiben):

Verfügbarkeit, z. B.

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß eines getesteten Konzepts
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage z. B. DDOS, höhere Gewalt)
- Dokumentation von Syntax und Semantik der gespeicherten Daten
- Redundanz von Hard- und Software sowie Infrastruktur
- Umsetzung von Reparaturstrategien und Ausweichprozessen
- Vertretungsregelungen für abwesende Mitarbeiter

Welche Maßnahmen wurden getroffen (Bitte beschreiben):
Belastbarkeit der Systeme, z. B. • Dokumentation der Ursprungsdaten und ihrer Herkunft • Nachvollziehbarkeit der Verarbeitungsschritte
Welche Maßnahmen wurden getroffen (Bitte beschreiben):
Verfahren zur Wiederherstellung der Verfügbarkeit pers.-bez. Daten nach einem physischen oder technischen Zwischenfall, z. B. • Erstellung und Umsetzung eines Notfallkonzepts • Erarbeitung eines Notfallhandbuches • Integration des Notfallmanagements in Geschäftsprozesse • Durchführung von Notfallübungen • Erprobung von Wiederanlaufszenarien
Welche Maßnahmen wurden getroffen (Bitte beschreiben):
Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen, z. B. • regelmäßige Revision des Sicherheitskonzepts • Information über neu auftretende Schwachstellen und andere Risikofaktoren, ggf. Überarbeitung der Risikoanalyse und -bewertung • Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme • externe Prüfungen, Audits, Zertifizierungen
Welche Maßnahmen wurden getroffen (Bitte beschreiben):

9. Auftragsverarbeitung durch Dritte (Art. 28 Abs. 1 DS-GVO)

☐	Gem. Art. 28 Abs. 1 DS-GVO findet eine Auftragsverarbeitung statt.
☐	Liegt eine schriftliche Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DS-GVO vor?
Name des Auftragsver-arbeiters	
Standort	

10. Anlagen

Es liegen folgende Unterlagen schriftlich vor:

☐ Rollen- und Berechtigungskonzept
☐ Dienstanweisungen/Dienstvereinbarungen
☐ Datensicherungskonzept
☐ Managementbewertungen
☐ Wiederanlaufpläne/-konzept
☐ Zertifikate
☐ Risikobehandlungspläne
☐ Richtlinien
☐ Sicherheitskonzept
☐ Sonstiges (bitte unten ergänzen)

Unterschrift:

Datum: