Datenschutz-Konzept

gemäß DSGVO und Datenschutz-Anpassungsgesetz 2018

„Elternverein RG Lambach“

ZVR-Zahl des Vereins gemäß § 18 Abs. 3: **657572855**

Lambach, am 19.04.2018

1 Allgemeine Angaben

1.1 Datenschutz-Konzept

Dieses Datenschutzkonzept beruht auf den in Art 5 Z 1 DSGVO formulierten Grundsätzen wie Zweckbindung, Datenminimierung, Speicherbegrenzung sowie Integrität und Vertraulichkeit und ist rechtmäßig (Art 6 DSGVO). Die von der DSGVO geforderte Einhaltung der Verordnungskonformität (Art. 5 Z 2; Art 24 Z 1), der Einhaltung der Betroffenenrechte (Art 13-20), der Meldepflicht bei Datenschutzverletzung (Art 33-34), der Nachweis- und Rechenschaftspflicht (Art 5 Z 2, Art 24 Z 1) ist gewährleistet. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt (Art 32 Z 1).

1.2 Sachliche und räumliche Tätigkeit

Unser Kleinverein * verarbeitet personenbezogene Daten von natürlichen Personen und Schulkinder im Sinne des Art 8 DSGVO ganz oder teilweise automatisiert und hat seine Niederlassung in der EU, **in 4650 Lambach**

* *Außerdem werden die Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung der DSGVO die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen. Für die Definition des Begriffs „Kleinstunternehmen sowie kleine und mittlere Unternehmen“ sollte Artikel 2 des Anhangs zur Empfehlung 2003/361/EG der Kommission maßgebend sein.*

Referenzen: Art 2 + 3 + 4 DSGVO, EuGH Entscheidung Weltimmo v. NAIH (C-230/34)

1.3 Datenschutzbeauftragter (DSB)

Trifft einer der nachfolgenden Kriterien zu, ist ein externer oder interner DSB notwendig und zu bestellen:

Kriterium	Ja	Nein
Verarbeitung der Daten durch eine Behörde oder eine öffentliche Stelle, mit Ausnahme der Gerichte		X
Verarbeitung der personenbezogenen Daten stellt eine Kerntätigkeit der Organisation dar und/oder erfordert eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person		X
Verarbeitung besonders schutzwürdige Kategorien personenbezogenen Daten (Art 9 Z 1 DSGVO wie zB Gesundheitsdaten, ethische Herkunft, genetische bzw. biometrische Daten, Gewerkschaftszugehörigkeit, usw.) stellt eine Kerntätigkeit der Organisation dar		X

Referenzen: Art 37 DSGVO, Erwägungsgründe 97

Da für unseren Verein keiner der obigen Kriterien zutrifft, wird kein DSB bestellt.

1.4 Verantwortliche (Stammdaten)

Verantwortliche
Vorstand des Elternvereines RG Lambach

Referenzen: Art 4 Z 7 DSGVO

1.5 Weiterbildung und Stand der Technik

Betreffs Weiterbildung und Stand der Technik setze ich folgende Aktivität:

Aktivitäten	Veranstalter	sonstiges
Info- u. Weiterbildungsveranstaltungen	WKO online seminare	
Homepages bzw. Newsletter	http://www.dataprivacydoctors.at/	
	!!! DSGVO-Page der WKO !!!	

Referenzen: Art 4, 5-11 DSGVO

2 Datenverarbeitungen/Datenverarbeitungszwecke

2.1 Zwecke und Beschreibung der Datenverarbeitung:

2.1.1 Mitgliederverwaltung

Führung, Verarbeitung und Übermittlung von Mitgliederverzeichnissen, Evidenz der Mitglieds- und Förderungsbeiträge, Verkehr mit Mitgliedern oder Förderern von Körperschaften des öffentlichen und privaten Rechts, insbesondere Vereinen, und Personengemeinschaften, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten.

Verarbeitung und Übermittlung von Daten im Rahmen des Vereinszweckes, diese sind: die Erziehung und den Unterricht der Schule anvertrauten Kinder zu fördern, die schulbezogenen Interessen und Anliegen der Eltern und Kinder zu vertreten, bedürftige Schülerinnen und Schüler zu unterstützen, die Lebensqualität der Schüler im Schulalltag zu fördern, alle dem Elternverein gemäß den Bestimmungen des Schulunterrichtsgesetzes zustehenden Rechte wahrzunehmen, die Erziehungsberechtigten bei der Geltendmachung der ihnen nach dem Schulunterrichtsgesetz zustehenden Rechte zu unterstützen wie bei der Finanzierung und Organisation von Lehrmitteln, Unterrichtsmaterial, Kursen, schulischen Veranstaltungen u. dgl., sowie Geschäftsbeziehungen mit Lieferanten, sowie an den Vereinsaktivitäten mitwirkende Dritte inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

2.1.2 Kommunikation

Vereinszweck-orientierte Information und Betreuung von kategorisierten Mitglieder, Lieferanten, Förderern und an den Vereinsaktivitäten mitwirkende Schule sowie Dritte inkl. deren jeweiligen Kontaktpersonen und Interessenten einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter und Informationsmaterial.

2.2 Wurde eine Datenschutz-Folgenabschätzung durchgeführt?

Ja ☐ **Nein** **X**

Wenn Ja, wann?

Wenn Nein, aus welchem Grund nicht?

Eine Datenschutz-Folgenabschätzung ist nicht durchzuführen, da sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht – siehe Risikobewertung und Maßnahmen - ,da keine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt und da keine umfangreichen Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt. Es gibt auch keine Überwachung öffentlich zugänglicher Bereiche durch Video.

Ob für unsere Anwendungen eine Datenschutz-Folgenabschätzung gesetzlich vorgeschrieben bzw. nicht vorgeschrieben ist, kann nicht gesagt werden, da diese Listen seitens der Datenschutzbehörde noch nicht vorliegen (Art 35 Z4 + Z5)

Referenzen: Art 35 Z1-3 DSGVO

3 Verfahrensverzeichnis

Referenzen: Art 30, Art 31 DSGVO, Erwägungsgründe 13, 75, 76, 82, 89

3.1 Mitgliederverwaltung

3.1.1 Verantwortliche

Verantwortliche	Für Datenschutz zuständig
Vorstand des Elternverein RG Lambach	Vorstand des Elternverein RG Lambach

3.1.2

3.1.3 Zweck

Führung, Verarbeitung und Übermittlung von Mitgliederverzeichnissen, Evidenz der Mitglieds- und Förderungsbeiträge, Verkehr mit Mitgliedern oder Förderern von Körperschaften des öffentlichen und privaten Rechts, insbesondere Vereinen, und Personengemeinschaften, einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z. B. Korrespondenz) in diesen Angelegenheiten.

Verarbeitung und Übermittlung von Daten im Rahmen des Vereinszweckes, (Vereinszweck, siehe Punkt 2.1.1) wie bei der Finanzierung und Organisation von Lehrmitteln, Unterrichtsmaterial, Kursen, schulischen Veranstaltungen u. dgl., sowie Geschäftsbeziehungen mit Lieferanten, sowie an den Vereinsaktivitäten mitwirkende Schule sowie Dritte inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie zB Rechnungen, Korrespondenzen oder Verträge) in diesen Angelegenheiten

3.1.4 Kategorien der betroffenen Personen

Lfd.Nr.	Beschreibung der Kategorien betroffener Personen
1	Vereinsmitglieder und deren Kinder
2	Funktionäre
3	Förderer inkl. Kontaktpersonen
4	An den Vereinsaktivitäten mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen

3.1.5 Rechtsgrundlagen

- Art 6 Z 1 lit a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen) DSGVO
- § 132 BAO

- §§ 190, 212 UGB
- EStG, UStG
- Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: BGBl. II Nr. 312/2004
- Vereinsgesetz 2002

3.1.6 Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Unterlagen zu aufrechten Vereinstätigkeit, Geschäftsabwicklungen, Mitgliedsbeiträge, Rechnungen, erledigte Geschäftsfälle, Unterlagen und Zustimmungserklärungen sowie Verträge mit Auftragsverarbeitern * sind im Archiv abgelegt.

** Bank verarbeitet die Daten ihrer Kunden als Verantwortlicher im Sinne der Datenschutzgrundverordnung (DSGVO) und nicht als Auftragsverarbeiter. Es muss daher mit in Kraft treten der DSGVO (25.5.2018) keine gesonderten Auftragsverarbeitung nach Art 28 DSGVO mit dem Verein abgeschlossen werden. Bei Überweisungsaufträgen wird lediglich der IBAN des Empfängers auf Kohärenz geprüft und der Überweisungsauftrag ausgeführt. Die Empfängernamen, die in einen Überweisungsauftrag eingegeben werden, werden nicht im Sinne des Art 4 DSGVO verarbeitet und dienen dem Verein lediglich zu Dokumentationszwecken, damit dieser seine Zahlungen zuordnen kann.*

3.1.7 Kategorien der verarbeiteten Daten

- Vorlage ist SA003 Mitgliederverwaltung (https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003495&FassungVom=2018-05-24)

Betroffene Personengruppen:	Nr.:	Datenkategorie:	Empfängerkategorie
Alle	01	Einwilligung nach Art 4 abgelegt	3, 4
Mitglieder und deren Kinder	02	Mitgliedsnummer / Ordnungsnummer	2 - 6
	03	Name oder Bezeichnung der Organisation, Firma	1 - 6
	04	Anrede / Geschlecht	1 - 6
	05	Geburtsdatum	2 -5
	06	Anschrift	1 -6
	07	Telefon-, Faxnummer Email und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	2 - 5 (Newsletter Sperre)
	08	Beruf oder Branche (nach Angabe des Betroffenen)	2 - 5
	09	Mitgliederkategorie, z. B. ordentliches/außerordentliches/unterstützendes Mitglied, Ehrenmitglied usw.	1 - 6
	10a	Name des/der schulpflichtigen Kindes/er sowie Klasse	3, 4
	10b	Fotos der Mitglieder sowie deren Kinder für die homepage (Einwilligung des Erziehungsberechtigten, siehe Anhang)	3, 4
	11	Eintritts-, Austrittsdaten	2 - 6
	12	Beiträge	1 - 6

	13	Vereinszweckrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen	2 - 5
	14	Angaben betreffend die Inanspruchnahme von Leistungen des Auftraggebers mit Zahlungsverpflichtungen des Betroffenen an den Auftraggeber	2 - 5
	15	Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen	1 - 6
	16	Bankverbindung1 - 6	1 - 6
Funktionäre:	17	Ordnungsnummer wie zB Mitgliedernummer, ...	2 – 6
	18	Name	1 – 6
	19	Anrede / Geschlecht	1 – 6
	20	Geburtsdatum (Volljährigkeit)	2 - 5
	21	Zustellanschrift im Rahmen der Funktion	1 - 6
	22	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben, beim Auftraggeber	1 - 6
	23	Funktion beim Auftraggeber	2 – 6
	24	Beginn und Ende der Funktion	2 - 6
	25	Zahlungsverpflichtungen des Betroffenen an den Auftraggeber	1 -6
	26	Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen	1,-6
Förderer inklusive Kontaktpersonen	27	Ordnungsnummer	2- 6
	28	Name oder Bezeichnung der Organisation und Firmenbuch- und andere Kennzahlen (UID-Nummer, ...)	1 -6
	29	Anrede/Geschlecht	2 - 6
	30	Anschrift	1 -6
	31	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	2 - 6
	32	Spenden und sonstige Leistungen des Betroffenen	1 -6
	33	Angaben betreffend die Inanspruchnahme von Leistungen des Auftraggebers	2 -6
	34	Zahlungen oder sonstige Leistungen des Auftraggebers an den Betroffenen	1 -6
	35	Kontaktperson	2 -6
	36	Deren Adresse sowie Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergebende Kontakdaten	1 - 6

		der Kontaktperson	
mitwirkende Dritte und Lieferanten inkl. Kontaktpersonen	37	Ordnungsnummer Lieferantennummer, ...	2 - 6
	38	Name oder Bezeichnung der Organisation und Firmenbuch- und andere Kennzahlen (UID-Nummer, ...)	1 -6
	39	Anrede/Geschlecht	1 -6
	40	Anschrift	1 -6
	41	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	2-6
	42	Vereinszweckrelevante Aktivitäten bzw. Veranstaltungen	2 - 5
	43	Bankverbindungen	1 -6
	44	Namen Kontaktpersonen	1 -6
	45	Zuordnung zu einer bestimmten Kategorie (einschließlich regionale Zuordnung, usw.)	2 - 5
	46	Vertragstext und Geschäftskorrespondenzen, Rechnungen,..	2 - 6
	47	Besondere Rabatte bzw. Vergünstigungen, … für Schüler	2 -6
	48	Gegenstand der Lieferung oder Leistung	1 -6
	49	Rechnungsbetrag	1 -6

3.1.8 Löschungs- und Aufbewahrungsfristen

Daten (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1 - 18, 20 – 30,	Bis zur Beendigung der Mitgliedschaft des Betroffenen und Ablauf der für den Auftraggeber geltenden Verjährungs- und gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden.
32 – 42	Bei Förderern: Bis zum Ablauf des dritten Jahres nach dem letzten Kontakt mit dem Auftraggeber.
43 - 55	Bis zur Beendigung der Geschäftstätigkeit mit Betroffenen und Ablauf der für den Auftraggeber geltenden Verjährungs- und gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; ferner bis zur Beendigung von Rechtsstreitigkeiten, bei denen die Daten als Beweis benötigt werden.
19, 31, 42, 56	Newsletter: Recht auf Widerspruch (Art 21 DSGVO)

3.1.9 Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

Nr.	Empfängerkategorien	Drittstaat außerhalb der EU	Internationale Organisation
1	Banken	Nein	Nein
2	Behörden und sonstige Institutionen auf Grund	Nein	Nein

	gesetzlicher Melde- oder Berichtspflichten wie, insbesondere Vereinsbehörden, Veranstaltungsbehörden usw.;		
3	Personen und Institutionen (Schule) auf Grund einer Ermächtigung oder Verpflichtung zur Datenübermittlung in den Statuten oder auf Grund besonderer Zustimmung des Betroffenen;	Nein	Nein
4	Rechtsanwälte, Gerichte und sonstige Stellen, zum Zweck der Rechtsdurchsetzung.	Nein	Nein
6	Steuerberater, Bilanzbuchhalter	*Nein*	*Nein*

3.1.10 Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten

3.2 Kommunikation

3.2.1 Verantwortliche

Wenn nicht die/der Obfrau/-mann auch die Verwaltungsarbeit des Vereines macht, so sollte die Person, die die pb Daten verwaltet/verarbeitet als für den Datenschutz Zuständige hier erwähnt werden

Verantwortliche	Für Datenschutz zuständig
Vorstand des Elternvereines RG Lambach	**Vorstand des Elternvereines RG Lambach**

3.2.2

3.2.3 Zweck

Vereinsorientierte Information und Betreuung von kategorisierten Mitglieder, Funktionären, Förderern und an den Vereinsaktivitäten mitwirkende Schule sowie Dritte inkl. deren jeweiligen Kontaktpersonen einschließlich automationsunterstützt erstellter und archivierter Textdokumente (wie z.B. Korrespondenz) sowie Übermittlung von Newsletter und Informationsmaterial.

3.2.4 Kategorien der betroffenen Personen

Lfd.Nr.	Beschreibung der Kategorien betroffener Personen
1	eigene Mitglieder und deren Kinder, Funktionäre, Förderer, Vereinstätigkeiten mit-wirkende Schule sowie Dritte
2	Kontaktpersonen von oben

3.2.5 Rechtsgrundlagen

- Art: 6 Z 1 lit a (Einwilligung der Betroffenen), b (zur Vertragserfüllung erforderlich), c (gesetzliche Verpflichtungen nach der BAO und dem UGB), f (berechtigte Interessen des Verantwortlichen)
- § 151 GewO 1994
- „SA022 Kundenbetreuung und Marketing für eigene Zwecke“ siehe Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004) StF: BGBl. II Nr. 312/2004
- Vereinsgesetz 2002

3.2.6 Verträge , Zustimmungserklärungen oder sonstige Unterlagen

Zustimmungserklärungen bzw. Verträge sowie Verträge mit Auftragsverarbeitern usw. sind im Archiv abgelegt.

3.2.7 Kategorien der verarbeiteten Daten

- Vorlage ist die Standardanwendung „SA022 Kundenbetreuung und Marketing für eigene Zwecke“

- Kategorien der verarbeiteten Daten und ob sie an welchen Empfänger übermittelt werden sind auf Grund **der konkreten Prüfung gemäß Datenminimierung nach Art 5 Z 1 DSGVO für unseren Verein mit (X)** angekreuzt.

Kategorien der betroffenen Personengruppe	Lf. Nr.:	Datenkategorien	Art 9 und Art 10 DSGVO	nlassfallRechtsvertreter	im AnlassfallGericht
1. eigene Mitglieder, Funktionäre, Förderer, Geschäftsabwicklung mitwirkende Schule sowie Dritte	01	Mitgliedernummer sonstige Ordnungszahlen	*Nein*	X	X
	02	Name bzw. Bezeichnung	*Nein*	X	X
	03	Anrede/Geschlecht	*Nein*	X	X
	04	Anschrift bzw. Lieferadresse	*Nein*	X	X
	05	Telefon- und Faxnummer und andere zur Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben	*Nein*	X	X
	06	Homepage, Soziale Netzwerke	*Nein*	X	X
	07	Einwilligung nach Art 4 abgelegt	*Nein*	X	X
	08	Berufs-, Branchen- Geschäftsbezeichnung	*Nein*	X	X
	09	Firmenbuch- und andere Kennzahlen (UID-Nummer, ...)	*Nein*	X	X
	11	Vom Betroffenen bekannt gegebene Interessen und Spezialgebiete	*Nein*	X	X
	12	Vereinszweckrelevante Aktivitäten, insb. Teilnahme an Veranstaltungen	*Nein*	X	X
	13	Interessen (auf Grund bisherigen Teilnahme oder eigener Angaben des Vereinsmitgliedes gegenüber dem Auftraggeber)	*Nein*	X	X
	14	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*	X	X
Kontaktpersonen von oben	15	Name bzw. Bezeichnung, Anrede/Geschlecht	*Nein*	X	X
	16	Anschrift	*Nein*	X	X
	17	Telefon- und Faxnummer und andere zur	*Nein*	X	X

		Adressierung erforderliche Informationen, die sich durch moderne Kommunikationstechniken ergeben			
	18	Funktion oder betreutes Aufgabengebiet	*Nein*	X	X
	19	Einwilligung nach Art 4 abgelegt	*Nein*	X	X
	20	Auftragssperre = Recht auf Einschränkung geltend gemacht	*Nein*	X	X

3.2.8 Löschungs- und Aufbewahrungsfristen

Daten (Lfd. Nr.)	Angabe bzw. Beschreibung der Löschungs- bzw. Aufbewahrungsfristen
1 – 22	Aufgrund der gesetzlichen Aufbewahrungsfristen wie zB § 132 Abs 1 BAO, §§ 190, 212 UGB, § 18 UStG Abs 2 Z3 auf jeden Fall 7 Jahre; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen

3.2.9 Kategorien der Empfänger sowie Übermittlungsort (Drittstaat, Internationale Organisation)

Empfängerkategorien	Drittstaat (d.h. Staaten außerhalb der EU)	Internationale Organisation
1.Rechtsvertreter im Anlassfall	Nein	Nein
2.Gericht im Anlassfall	Nein	Nein

3.2.10 Dokumentation der getroffenen geeigneten Garantien im Falle einer Übermittlung in Drittstaaten die nicht auf Art 45, 46, 47 oder 49 Z 1 Unterabsatz 1 DSGVO erfolgt

Es erfolgt keine Übermittlung an Drittstaaten.

4 Checkliste - IT-Safe (WKO)

Wir sind die wirklich hilfreiche IT-Checkliste für EPUs unter https://itsafe.wkoratgeber.at/ durch gegangen und konnten feststellen, ob und wo es in unserem Kleinverein Probleme im IT-Bereich geben könnte. Die daraus folgenden Maßnahmen finden sich unter TOMs und werden bis zum 24. Mai 2018 umgesetzt sein.

5 Impressum und Statuten

Siehe veröffentlichung auf unserer Homepage : https://elternvereinrglambach.jimdo.com/

6 Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

6.1 Selbstschutz

Wir versuchen unser Such- und Surfverhalten soweit wie möglich sicher zu gestalten zu halten und verwende daher zB den europäischen Open Source Browser https://cliqz.com/ inklusive Ghostery (verhindert und zeigt uns die Trackingversuche) oder https://pi-hole.net/ und die europäische Suchmaschine: https://www.startpage.com/ statt Google.

1. Schritt: Backup auf einen USB-Stick
2. Schritt: kontrollieren ob Backup funktioniert
3. Schritt: Verschlüsseln mittels Passwort

6.2 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

i. Risikoanalyse
ii. Datenschutzfreundliche Voreinstellungen
iii. Weiterbildung
iv. Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, sichere und verschlüsselte Speicherung und Übertragung, (zB. Ob Datenschutzbeauftragter und/oder Dokumentation nach DSGVO vorhanden, Vorabüberzeugungspflicht, Nachkontrollen)
v. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt:

Jahr	Ergebnisse der Überprüfung, Bewertung und Evaluierung
2019	
2020	

Referenzen: Art 32 Z 1 DSGVO
Quelle 6.2 bis 6.9 : https://www.datenschutz-guru.de/files/**Ausfuellhilfe_TOM_9_BDSG_V2**.docx

7 Betroffenenrechte wahren

Grundsätzlich stelle wir jedem Nutzer bzw. Betroffenen die jeweils aktuelle Version dieses Datenschutzkonzeptes auf unser Homepage unter. https://elternvereinrglambach.jimdo.com/ zum Downloaden zur Verfügung.

Gemäß der DSGVO hat jeder Betroffene folgende Rechte:

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Einschränkung (Art 18 DSGVO)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Recht auf Widerspruch (Art 21 DSGVO)
- Recht auf Beschwerde bei der Datenschutzbehörde

7.1 Prozesse betreffs Betroffenenrechte

i. Ich erhalte Kenntnis dass ein Betroffener seine Rechte geltend machen will, sei es zB mündlich, schriftlich. per Email
ii. Sollte der Betroffene mir nicht persönlich bekannt sein, so muss ich zwecks Vermeidung einer Datenschutzverletzung die Identität des Antragsstellers (Betroffenen) feststellen:
„Sehr geehrte Frau/Herr …!
Da ich Sie leider noch nicht persönlich kennen lernen durfte, bitte ich Sie, um keine Datenschutzverletzung zu machen wie zB pb Daten an eine falsche Person weiterzuleiten, mir eine Kopie/Scann Ihres Personalausweises/Reisepasses zu kommen zu lassen.
Ich danke Ihnen für Ihr Verständnis
P.S.: Unser aktuelles Datenschutzkonzept unter https://elternvereinrglambach.jimdo.com/

iii. Identität kann nicht zweifelsfrei festgestellt werden und der Betroffene meldet sich trotz Information darüber nicht mehr: => Keine Aktivitäten meinerseits sind notwendig..
iv. Identität zweifelsfrei festgestellt und Anfrage ist rechtens:
=> Der Betroffene bekommt gemäß Art 19 DSGVO innerhalb von maximal 14 Tagen abhängig von seiner Anfrage in klarer und verständlicher Sprache folgende Antworten:

- Recht auf Auskunft (Art 15 DSGVO)
  Der Betroffene bekommt
  - den Link:https://elternvereinrglambach.jimdo.com/
  - sein Stammdatenblatt mit alle pb Daten (ScreenShot)
- Recht auf Berichtigung (Art 16 DSGVO)
  Der Betroffene bekommt
  - den Link: https://elternvereinrglambach.jimdo.com/
  - sein Stammdatenblatt mit den berichtigten pb Daten (ScreenShot)
- Recht auf Löschung (Art 17 DSGVO)
  Der Betroffene bekommt
    - den Link: https://elternvereinrglambach.jimdo.com/
    - sein Stammdatenblatt ohne pb Daten (ausgenommen Name) als Nachweis, dass die Löschung erfolgt ist mit den Hinweis, dass

▪ nach Kopie des Stammdatenblattes auch das ganze Stammdatenblatt inklusive Namen unwiderruflich gelöscht wurde (ScreenShot)

oder

  - Bei einem bestehenden oder abgeschlossenem Vertrag mit dem Betroffenen werde ich alle Daten, bis auf jene wo ich nach Art 6 Z 1 lit f ein berechtigte Interessen des Verantwortlichen DSGVO (vor allem Buchhaltungsunterlagen) geltend machen kann, löschen und daher aufgrund der gesetzlichen Aufbewahrungsfristen diese Daten auf jeden Fall erst nach 7 Jahre löschen; darüber hinausgehend bis zur Beendigung eines allfälligen Rechtsstreits, fortlaufender Gewährleistungs- oder Garantiefristen die pb Daten löschen. In diesen Fällen tritt an Stelle einer Löschung der Daten eine Sperrung (Einschränkung).

- Recht auf Einschränkung (Art 18 DSGVO)
  Der Betroffene bekommt
  - den Link https://elternvereinrglambach.jimdo.com/
  - sein Stammdatenblatt, dem er entnehmen kann, dass bei „Recht auf Einschränkung geltend gemacht“ ein Hackerl gesetzt ist und somit keine Verarbeitung seiner pb Daten erfolgt. (ScreenShot)
- Recht auf Übertragbarkeit (Art 20 DSGVO)

Der Betroffene bekommt den Link:

  - https://elternvereinrglambach.jimdo.com/
    - sein Stammdatenblatt mit alle pb Daten (ScreenShot)
    - gemäß Art 20 Z2 DSGVO übermittle ich sein Stammdatenblatt mit alle pb Daten als Cc.. sicher und verschlüsselt an einen anderen Verantwortlichen, den der Betroffene mir genannt hat
- Recht auf Beschwerde bei der Datenschutzbehörde

7.1.1 Profiling light

Wir verarbeiten (siehe Verfahrensverzeichnis Marketing) teil-automatisiert auch personenbezogener Daten von natürliche Personen, um Art und Form der jeweilig in Anspruch genommenen Vereins-Dienstleistung/Produkt, Interessen, Ort, Branche, …, Teilnahme an und Bereitschaft für Vereinsaktivitäten … zu kategorisieren und um im berechtigtes Interesse eine zielgerichtete Information und Betreuung (= simples Mitglieder/Fördere-Profil) sowie um eine personalisierte Information (siehe Newsletter) für unsere Mitglieder, Funktionäre, Förderer, Projektpartner zu ermöglichen.

Da nur eine teil-automatisiert, keine umfassende Bewertung persönlicher Aspekte natürlicher Personen, keine Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten erfolgt und auch ausdrücklich damit keinerlei automatische Generierung von Einzelentscheidungen verbunden ist und es gänzlich ohne rechtliche oder ähnliche Wirkung für den Betroffenen ist, ist dies Verarbeitung daher nicht als Profiling im Sinne des DSGVO (siehe unten Referenzen), sondern als **Profiling light, als Mitglieder- und Vereinszweck-orientiertes Service** zu sehen und es bedarf darüber hinaus auch keiner Datenschutz-Folgeabschätzung.

Referenzen: Art 4, Art 8, Art 9 DSGVO; Erwägungsgründe: 26ff, 51ff; § 4 Abs 4 DSGVO 2018

7.2 Meldung von Datenschutzverletzungen

Die DSGVO definiert in Art 33 eine „Verletzung des Schutzes personenbezogener Daten“ (Databreach) als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

i. Ich, als Datenschutz Zuständige, erlange Kenntnis von einer Datenschutzverletzung.
ii. **Innerhalb von 72 Stunden** mache ich eine Meldung mit Hilfe des „Muster Datenschutzverletzung“ (siehe Anhang) an die gemäß Art 55 DSGVO zuständige Aufsichtsbehörde, wenn die Verletzung des Schutzes pb Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
iii. Gemäß Art 34 Z3 DSGVO muss keine Benachrichtigung der Betroffenen erfolgt, da die Verletzung des Schutzes pb Daten aufgrund meiner TOMs (zB Verschlüsselung in Rest und Motion, BackUp, …) voraussichtlich kein **hohes Risiko** für deren persönlichen Rechte und Freiheiten zur Folge hat
iv. Die Datenschutzbehörde ist wohlbegründet gegenteiliger Meinung und fordert mich auf, alle/gewisse Betroffenen zu informieren, siehe Art 34 Z4 DSGVO.
i. Ich informiere Betroffenen umgehend mit einer entsprechenden Variation des „Muster Datenschutzverletzung“ (siehe Anhang)
v. Ich werde alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht, siehe Art 33 Z5 DSGVO.

8 Risikoanalyse

Referenzen: Art 24 + 25 DSGVO, Erwägungsgründe: 74-78, 81

8.1 Schutzbedarfsanalyse

Unsere Vorabanalyse ergab, dass es sich bei folgende pb Daten der Mitglieder, Funktionäre, Förderer, Lieferanten, Geschäftspartner und an der Geschäftsabwicklung mitwirkende Dritte inkl. der jeweiligen Kontaktpersonen um Daten mit vernachlässigbaren bis geringem Schutzbedarf handelt, da. sowohl aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht und auch allgemeine TOMs gemäß DSGVO gesetzt wurden:

Öffentlich zugängliche Daten, Ordnungsnummer, Name, Firma oder sonstige Geschäftsbezeichnung, Anrede/Geschlecht, Anschrift, Homepage, Kontaktdaten (Tel., Mail, Fax,), Berufs-, Branchen- und Geschäftsbezeichnung, Firmenbuchdaten, Keine Zusendungen von Werbematerial, Newsletter erwünscht, Kenn-Nummern für Zwecke amtlicher Statistik wie UID-Nummer und Intrastat-Kenn-Nummer, Korrespondenzsprache, Namen der Kontaktpersonen, Kontaktdaten der Kontaktpersonen (Tel., Mail, Fax, Anschrift odgl.), Funktion/Rolle der Kontaktperson,

8.2 Risikoanalyse ohne Maßnahmen

Schutzziele für unsere Risikobewertung nach Art 4 Z 12 sind: Vertraulichkeit, Integrität und Verfügbarkeit. Die Risiko-Bewertung erfolgt nach „Schwere“ und „Eintrittswahrscheinlichkeit (EWK)“, siehe unten

Folgende Daten wurden analysiert und in die entsprechenden Kategorien eingetragen:

Kategorie	pb Daten
1	Name, Adresse, Fotos usw. der Kinder Art 8 DSGVO
2	Missbrauch von Geldern
3	Datenverlust durch techn. Fehler
4	Pb Daten mit vernachlässigbaren bis begrenzten Schutzbedarf, siehe oben Vorabanalyse

Schwere				
Existenzgefährdend				1
Wesentlich				

Begrenzt				**4**	
Vernachlässigbar					
	Vernachlässigbar	Möglich	Sehr wahrscheinlich	Garantiert	**EWK**

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

Folgen ohne Maßnahmen:

Data Breach		
Kein Risiko	**Risiko**	**Hohes Risiko**
		• Datenschutzbehörde **UND** Betroffene informieren •Folgeabschätzung notwendig

8.2.1 Bewertungsmaßstäbe

Schwere:

Schwere	Auswirkung auf Betroffene	Folgen überwinden	Beispiele
Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlichkeiten	Unannehmlichkeiten sollten sich beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, …
Begrenzt	Wesentliche Unannehmlichkeiten	Unannehmlichkeiten sollten sich – trotz Schwierigkeiten – überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, …
Wesentlich	Wesentliche Folgen	Unannehmlichkeiten sollten sich – trotz großer Schwierigkeiten – überwinden lassen	Kontaktaufnahme der Kinder durch Unbefugte zB per Email Kategorien und Klassifizierungen werden bekannt, Missbrauch von Geldern, Vorladungen, Verschlechterung eines Verhältnisses, Weitergabe der Passwörter,
existenz-gefährdend	Irreversible Folgen	Irreversible Folgen kaum bzw. nicht überwindbar	Ansprechen der Kinder mit Vorname am Schulweg, .. durch Unbefugte Identitätsdiebstahl; … langfristige Beschwerden, …

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

Eintrittswahrscheinlichkeit:

EWK	Wahrscheinlichkeit	Beispiele
Vernachlässigbar	0-24% Wahrscheinlichkeit	zB Diebstahl von Unterlagen aus einem Safe
Möglich	25-69% Wahrscheinlichkeit	Zb gezielter und koordinierter Angriff durch einen Hacker, Verlust des Hardware bzw. pb Daten durch Diebstahl oder durch fahrlässiges Handeln
Sehr wahrscheinlich	70-99% Wahrscheinlichkeit	zB Eindringung eines Schädigungs-Mails,
Garantiert	100% Wahrscheinlichkeit garantiert	zB Ausfall durch einen Festplattenausfall, Datenverluste durch technische Fehler

Quelle: WIFI-Unterlagen zum zertifizierten Datenschutzbeauftragten

8.3 Maßnahmen

Siehe TOMs

8.3.1 Vertraulichkeit

i. **Zutrittskontrolle:** Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen mit Schlüssel
i. **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung mit Kennwörter, automatische Sperrmechanismen
i. **Zugriffskontrolle**: Zugriff nur durch Verantwortlichen

8.3.2 Integrität

i. **Eingabekontrolle**: Personenbezogene Daten in das Datenverarbeitungssysteme werden ausschließlich vom Verantwortlichen eingegeben, verändert oder entfernt, Dokumentenmanagement

8.3.3 Verfügbarkeit

i. **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, Virenschutz, Firewall, Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen an einem sicheren Ort

ii. Rasche **Wiederherstellbarkeit**: Backup mindestens wöchentlich

8.4 Risikoanalyse

Schwere					
Existenzgefährdend					
Wesentlich					
Begrenzt		**1**			
Vernachlässigbar	**4**				
	Vernachlässigbar	Möglich	Sehr wahrscheinlich	Garantiert	**EWK**

8.5 Folgen der Maßnahmen betreffs Risiko

Data Breach		
Kein Risiko	**Risiko**	**Hohes Risiko**
	• Datenschutzbehörde informieren	
•Mitglieder, Betroffene sind nicht zu informieren •Keine Folgenabschätzung notwendig		

Aufgrund der gesetzten TOMs muss bei einem DataBreach die betroffenen Mitglieder bzw. Personen nicht informiert werden, nichts desto trotz wird die Behörde bei DataBreach mit Risiko für pb Daten der Kategorie 1 informiert.

Referenzen: Art 22 + 35 DSGVO, Erwägungsgründe: 76, 84 und 89 – 93, Working Paper 240 der Art 29 Gruppe

9 Zusammenfassung und GV-Beschluss

Wir sehe das hier dokumentierte Datenschutzniveau mit den gesetzten TOMs für uns als Kleinverein (siehe Allgemeiner Teil) auch aufgrund unserer finanziellen, technischen und organisatorischen Beschränkungen als **angemessen und ausreichend** an.

Liebe Mitglieder!

Vertrauen zwischen den Vereinsmitgliedern und den Funktionären ist die Grundlage und Voraussetzung für unsere Vereinstätigkeit, daher sind auch alle Ihre persönlichen und beruflichen Daten und die Ihrer Kindern bei uns in guten Händen.

Wir sichern Ihnen zu, dass wir sorgsam und streng vertraulich damit umgehend und immer am aktuellen Stand der technischen und organisatorischen Datenschutz-Maßnahmen sind.

Das hier vorliegende Datenschutzkonzept unseres Vereines wurde von der Generalversammlung am 23. April 2018 mit 100% Stimmen dafür angenommen.

……Vorstand des Elternvereines RG Lambach……..

9.1 Muster Datenschutzverletzung (WKO)

Datenschutzverletzung

Art 33 EU-Datenschutzgrund-Verordnung (DSGVO) -
Meldung an die Aufsichtsbehörde:
Österreichische Datenschutzbehörde,
Hohenstaufengasse 3, 1010 Wien
E-Mail: dsb@dsb.gv.at

1. Name und Kontaktdaten des **Verantwortlichen**[1]**:**

   a. Name und Anschrift:

   b. E-Mail-Adresse, Tel.Nr.:

2. Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

soweit möglich Kategorien und ungefähre Zahl der **betroffenen Personen**:

   a. soweit möglich betroffene Kategorien und ungefähre Zahl der **personenbezogenen Datensätze**:

3. Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

4. Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

Siehe TOMs

   a. ggf **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

Siehe TOMs

5. **Datum und Uhrzeit** des Vorfalls:

1

☐ **Begründung**, falls die Meldung länger als 72h nach dem Vorfall erfolgte:

Lambach, am …….

…….
Unterschrift

10 Einwilligungserklärung – Eltern/Erziehungsberechtigte

„Elternverein RG Lambach“

Name des Erziehungsberechtigten:

Adresse:

Telefon:

Email:

Bitte kreuzen Sie als Erziehungsberechtigte an, ob Sie zustimmen oder nicht zustimmen.

Ja	Nein	Lambach, am_____
		Der gesetzliche Vertreter des/der betroffenen Schüler/Schülerin (Kinder nach Art 8 DSGVO) stimmt ausdrücklich zu, dass der Verein den Namen und die Klasse des/der Schülers/Schülerin verarbeiten darf: Name des/der Schülers/Schülerin : Klasse:
		Der gesetzliche Vertreter des/der betroffenen Schüler/Schülerin stimmt ausdrücklich zu, dass Fotos des/der Schülers/Schülerin (zB bei Vereins-Veranstaltungen) vom Verein verarbeitet und auf der vereinseigenen Homepage veröffentlicht werden dürfen.

Gemäß der DSGVO haben Sie als Betroffene jederzeit folgende Rechte, die Sie bitte per Email an die Datenschutz Verantwortliche des Vereines, (elternvereinrg@gmail.com) geltend machen können:

- Recht auf Auskunft (Art 15 DSGVO)
- Recht auf Berichtigung (Art 16 DSGVO)
- Recht auf Löschung (Art 17 DSGVO)
- Recht auf Einschränkung (Art 18 DSGVO)
- Recht auf Übertragbarkeit (Art 20 DSGVO)
- Recht auf Beschwerde bei der Datenschutzbehörde