Informationen zu Datenschutz und Informationssicherheit der Projektgruppe Nahwärme Erdbach

Datenschutz und Informationssicherheit – Warum?
Datenschutz und Informationssicherheit sind für uns aus zwei Gründen zentrale Themen:
Datenschutz schützt Menschen:
Maßnahmen zum Datenschutz schützen persönliche Informationen über die Mitarbeiter der Projektgruppe und der Teilnehmer zu der Befragung der Erdbacher Bürger.
Informationssicherheit schützt die Werte aller Beteiligten:
Maßnahmen zur Informationssicherheit schützen die Grundlagen der Projektgruppe und sind daher in unser aller Interesse.
Deswegen

- Schützen wir die personenbezogenen und vertraulichen Daten der Erdbacher Bürger.
- Gehen wir mit den Daten von Dritten mindestens genauso sorgfältig um, wie wir es uns für den Umgang mit unseren eigenen Daten wünschen.

Anwendung der DSVGO
Die Arbeitsanweisungen für den Umgang mit den Daten gemäß DSGVO sind bei der Leitung der Projektgruppe (Ortsbeirat) hinterlegt. Die Betroffenen sind entsprechend geschult.

Gespeicherte Daten und deren Nutzung

1. **Persönliche Daten der Erdbacher Bürger**
   Die persönlichen Daten der Erdbacher Bürger werden nur zu Zwecken der Projektgruppe genutzt.
   Unter anderem für:

- Infos über die Tätigkeiten der Projektgruppe
- Versendung von Informationsbroschüren
- **Zugriff auf die Daten** hat die Leitung der Projektgruppe (Ortsbeirat) und die Arbeitsgruppe Kommunikation / Öffentlichkeitsarbeit
- **Löschfristen** Auf Wunsch des Bürgers werden die persönlichen Daten
- spätestens nach einem Jahr gelöscht. Dies beinhaltet jedoch nicht die Namen, welche
- zu Zwecken der Chronik relevant sind.
- Die **Datenverwaltung** erfolgt durch die Arbeitsgruppe Kommunikation / Öffentlichkeitsarbeit.

Technische und Organisatorische Maßnahmen zum Datenschutz

- Pseudonymisierung und Verschlüsselung der Daten
- Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten.
- rasche Wiederherstellung von Daten und Zugängen nach einem Zwischenfall
- ein Verfahren „zur regelmäßigen Überprüfung, Bewertung und Evaluierung“ der Maßnahmen.

Breitscheid, den 17.12.2019

XXXXXXXXXXXXX
Zuständigkeits-Person
für die Datenverwaltung der Projektgruppe

Bemerkung: Um dem Genderwahnsinn im Text dieses Dokumentes zu entgehen, gelten alle auf Personen bezogenen Aussagen für alle Geschlechter

Arbeitsanweisung für den Umgang mit persönlichen Daten gemäß der Datenschutz Grundverordnung

Wie lauten unsere wichtigsten Regeln?

- Wir halten uns an geltendes Recht.
- Wenn wir Fragen haben oder Probleme erkennen, wenden wir uns an den direkten Vorgesetzten oder die Zuständigkeits-Person für die Datenverwaltung.
- Wir behandeln personenbezogene Daten vertraulich und geben Informationen nur an Berechtigte heraus.
- Wir schützen unsere IT-Systeme (auch Notebooks, Smartphones u.a.) vor Diebstahl, Beschädigung und unbefugter Benutzung.
- Wir melden sofort, wenn Geräte und/oder Daten abhandenkommen.
- Wir nutzen die IT-Infrastruktur nur im zulässigen Rahmen: Private Dateien und Informationen haben im geschäftlichen IT-Netzwerk nichts verloren.
- Wir versuchen Informationssicherheits- und Datenschutzprobleme niemals selbst zu beheben, sondern melden diese sofort.

Was gilt für Passwörter?

- Verwenden Sie immer verschiedene Passwörter für unterschiedliche Systeme und Dienste.
- Verwenden Sie sichere Passwörter aus mindestens 8, besser 10 Zeichen inklusiv Groß und Kleinschreibung, Ziffern, Buchstaben und Sonderzeichen.
- Ändern Sie Passworte regelmäßig
- Behandeln Sie Ihre Passwörter wie die PIN Ihrer Kreditkarte.
- Wenn Sie ein Passwort vergessen haben: Setzen Sie sich mit Ihrem Vorgesetzten in Verbindung

Denken Sie immer daran:

- Wenn jemand Ihre Zugangsdaten hat, kann er sich als Sie ausgeben. Egal, was er oder sie vorhat.
- -- Geben Sie Ihre Passwörter an niemanden weiter. **Niemals**. Auch nicht an die Kollegen oder Ihre Urlaubsvertretung.
- -- Verwenden Sie als Passwort keine Begriffe, die im Duden oder anderen Wörterbüchern stehen.
- -- Verwenden Sie keine Namen oder Geburtsdaten von Ihnen oder Angehörigen.
- -- Heften Sie Ihre Passwörter nicht an den Bildschirm, legen Sie sie nicht unter Ihre Schreibtischauflage und bewahren Sie sie sicher auf.

Was gilt am PC?

- Wenn Sie Ihren PC verlassen, sperren Sie ihn.

Weitergabe von Daten

Achten Sie darauf, wem Sie welche Daten weitergeben oder mündlich mitteilen. Beispielsweise kann schon eine telefonische Anfrage oder die Bitte eines Kollegen zu einer unbeabsichtigten Weitergabe vertraulicher oder personenbezogener Informationen führen. Prüfen Sie immer sorgsam, was Sie wem und in welchem Umfang weitergeben, indem Sie

- nicht spontan antworten, sondern erst hinterfragen und nur die Informationen
- weitergeben, die tatsächlich erforderlich sind.
- die Weitergabe von Informationen im Zweifelsfall mit Ihrem Vorgesetzten oder, wenn es um personenbezogene Daten geht, der Zuständigkeits-Person für die Datenverwaltung abklären.
- auf „Lauscher“ oder auch unfreiwillige Mithörer achten (z.B. in der Öffentlichkeit).
-

Erfassung von Daten

- Bei der Erfassung von Daten der Erdbacher Bürger ist die Angabe von Geburtsdaten und Bankverbindungen freiwillig. Sie sind für die Erfüllung des jeweiligen Vertrages nicht relevant.

Wie nutze ich das Internet sicher?

- Denken Sie beim Surfen daran, dass die Nutzung protokolliert wird und kontrolliert werden kann.
- Zur Sicherheit gibt es Zugriffseinschränkung durch Webfilter. Wenn Sie eine gefilterte Seite beruflich benötigen, wenden Sie sich an Ihren Vorgesetzten.
- Seien Sie misstrauisch bei unbekannten Webseiten.
-

Was gilt für soziale Netzwerke?

- Verhalten Sie sich in sozialen Netzwerken, z.B. Facebook oder Twitter immer mindestens so umsichtig, wie Sie es auch in der realen Welt tun würden. Vermeiden Sie beleidigende Äußerungen, weil sie sehr unangenehme Folgen für die Projektgruppe und Sie persönlich haben können.
- Teilen Sie nur Informationen, die Sie auch einem beliebigen Dritten mitteilen würden. Stellen Sie sich einfach vor, dass Sie sie ans Schwarze Brett bei uns oder im Supermarkt um die Ecke neben die Kasse hängen würden. Was da nicht stehen darf, gehört auch nicht auf Facebook & Co.
- -- Vermitteln Sie nicht den Eindruck, dass Sie offiziell für die Projektgruppe sprechen, außer Sie sind hierfür besonders bevollmächtigt. Bei Beiträgen im geschäftlichen Zusammenhang müssen Sie deshalb darauf hinweisen, dass Sie sich nur als Privatperson äußern.

Wie nutze ich E-Mails sicher?

- Schalten Sie den Abwesenheitsassistenten ein, bevor Sie länger nicht auf Ihre E-Mails zugreifen können.
- -- Nutzen Sie Ihre geschäftliche E-Mail-Adresse nur für geschäftliche Zwecke – nicht privat.
- -- Leiten Sie geschäftliche E-Mails niemals an private E-Mail-Konten weiter. Weder an Ihres, noch an andere.
- -- Versenden Sie vertrauliche Informationen per E-Mail nicht ungeschützt, sondern nur mit Passwort (z.B. als Word-Datei mit Passwort oder als verschlüsselte Zip-Datei).

Was hilft gegen Computer-Viren?

- Vorsicht beim Öffnen von E-Mails und ihren Anhängen – E-Mails mit Schadsoftware sind heutzutage professionell gestaltet und daher oft nicht als solche erkennbar.
- Die Aktualisierung der Antivirensoftware läuft an Ihrem PC und auf mobilen IT-Systemen automatisch. Darum brauchen Sie sich nicht zu kümmern. Melden Sie aber Alarme und ungewohnte Meldungen oder Effekte an Ihren Vorgesetzten.
- -- Laden Sie keine Dateien aus unbekannten und fremden Quellen herunter; seien Sie misstrauisch.
- -- Rufen Sie keine fragwürdigen Webseiten auf. Beschränken Sie sich am besten auf die beruflich benötigten Webseiten.

Wie nutze ich USB-Sticks und externe Speichermedien sicher?

- Der beste Schutz ist Verschlüsselung:
- Nutzen Sie ausschließlich von der Projektgruppe ausgegebene Speichermedien und beachten Sie deren Vorgaben.
- Gehen Sie sehr sorgfältig mit den Speichermedien um. Schützen Sie sie vor versehentlichem Verlust oder Diebstahl. Kommen Speichermedien abhanden (z.B. Handys, Laptops, USB-Sticks), melden Sie dies unverzüglich innerhalb von 72 Stunden– evtl. bestehen strenge gesetzliche Meldepflichten für die Projektgruppe.
- Geben Sie beschädigte Speichermedien immer an den Vorgesetzten zurück.
- -- Die Nutzung privater Speichermedien ist unzulässig.

Wie entsorge ich Daten?

- Papier, das personenbezogene oder vertrauliche Daten enthält, muss über Schredder oder andere sichere Methoden unlesbar gemacht oder in eine verschlossene Datentonne entsorgt werden.
- Digitale Daten müssen sicher gelöscht werden. Ein einfaches Verschieben in den „Papierkorb“ oder Löschen über den Windows Explorer ist nicht ausreichend. Einzelne Dateien sollten beispielsweise überschrieben werden, ganze Datenträger physikalisch zerstört werden.

Was muss ich über den Datenschutz wissen?

- Immer wenn Sie personenbezogene Daten bei anderen erheben oder einholen möchten, müssen Sie klären, ob Datenschutz-Informationen mitgeliefert werden müssen.
- Die Menschen, um deren personenbezogenen Daten es geht, haben eine Reihe von Rechten: auf Auskunft, Berichtigung, Löschung, Einschränkung der Datenverarbeitung, auf Datenübertragbarkeit und Widerspruch. Die Antwort auf dieses Begehren muss innerhalb eines Monats erfolgen.
- Wenn Daten durch einen Dritten verarbeitet werden (Outsourcing, Cloud-Computing), muss mein Arbeitgeber prüfen, ob eine Datenschutz-Vereinbarung mit dem Lieferanten oder Dienstleister (z.B. Bank) zu schließen ist. Wenn Sie sich nicht sicher sind, ob das gemacht wurde, fragen Sie Ihren Vorgesetzten
- Wird absichtlich oder unabsichtlich gegen den Datenschutz verstoßen (Datenpanne, Hacking, falsche Adressaten in E-Mail etc.), muss sofort der direkte Vorgesetzte innerhalb von 24 Stunden informiert werden! Dieser nimmt dann Kontakt mit der Datenschutzbeauftragten auf. Unter Umständen ist der Vorfall innerhalb von 72 Stunden der Aufsichtsbehörde zu melden – das wird nur gelingen, wenn alle zeitnah und richtig reagieren.
- Die Zuständigkeits-Person für die Datenverwaltung muss frühzeitig hinzugezogen werden, wenn neue Technologien und Prozesse zum Einsatz kommen.
- Die Zuständigkeits-Person für die Datenverwaltung überwacht und berät zu allen in dieser Arbeitsanweisung angesprochenen Themen – und natürlich auch zu allen anderen Fragen rund um den Datenschutz.
-

Ihre Zuständigkeits-Person für die Datenverwaltung :
Winfried Dörr (Mitarbeiter Projektgruppe Nahwärme Erdbach)

Arbeitsanweisung für die Erfassung persönlicher Daten

1. **Bei neuen Mitgliedern der Projektgruppe**
   Neue Mitglieder der Projektgruppe müssen unterschreiben, dass sie die mit den Zielen der Projektgruppe vollständig einverstanden sind. Um zielorientiert mit den Mitgliedern arbeiten zu können, benötigen wir von Ihnen die persönlichen Daten. Sofern vorhanden, akzeptieren Sie die Nutzung Ihrer Email Adresse.
   Geburtsdatum und Bankverbindung sind keine „Muss-Felder“ und somit freiwillige Angaben.
   Der Schriftführer der Projektgruppe archiviert und pflegt die persönlichen Daten.

2. **Bei der Datenerfassung der Erdbacher Bürger**
   Bei der Datenerfassung der Erdbacher Bürger werden entsprechende Fragebögen ausgegeben, in welchen die interessierten Bürger freiwillig ihre persönlichen Daten sowie die Daten ihrer Feuerungsanlagen und den Energieverbrauch eintragen und mit der Zusendung von Infos und Newslettern einverstanden sind. In diesen Fragebögen wird auf die Speicherung der Daten ausschließlich zu diesem Zweck hingewiesen und die Anerkennung muss mit Unterschrift bestätigt werden. Diese Daten werden vom Schriftführer in eine entsprechende Datenbank eingetragen.

Arbeitsanweisung für die Löschung persönlicher Daten

3. **Beim Ausscheiden eines Mitgliedes der Projektgruppe**
   Scheidet ein Mitglied der Projektgruppe durch Tod aus, oder wird die Mitgliedschaft von Ihm beendet, so werden die persönlichen Daten noch ein Jahr nach der Beendigung der Mitgliedschaft archiviert. Bei Kündigung der Mitgliedschaft erhält das Mitglied von der Projektgruppe innerhalb von 4 Wochen eine Bestätigung. Darüber hinaus dürfen die Namen der ausgeschiedenen Mitglieder zu Zwecken der Chronik weiterhin gespeichert bleiben.

Technische und Organisatorische Maßnahmen

a. **Leitlinien zur Informationssicherheit**
   Die Projektleitung ist verantwortlich für die Einhaltung der Datenschutz Grundverordnung (DSGVO).
   Die Projektleitung bestimmt die Zuständigkeits-Person für die Datenverwaltung
   Die Zuständigkeits-Person für die Datenverwaltung schult die jeweiligen Mitarbeiter und überwacht die Einhaltung der DSGVO.

b. **IT Benutzerrichtlinien**
   Unter „Gespeicherte Daten und deren Nutzung“ ist der Umgang und die Verantwortung für die Daten näher erläutert.
   Der Zugriff auf persönliche Daten ist, je nach Aufgabenbereich, limitiert.
   Die Datensicherung erfolgt mindestens 1 x pro Woche. Die Sicherheitskopie wird in einem Safe aufbewahrt. Der Datenträger wird immer wieder überspielt.
   WhatsApp sollte für die Übermittlung vertraulicher Informationen der Projektgruppe nicht genutzt werden.
   Vertrauliche Emails innerhalb der Leitung der Projektgruppe sollten verschlüsselt sein.

c. **Notfallplan**
   Sollten Datenträger, Handys, Laptops oder Speichermedien verloren gehen so ist der jeweilige Zuständigkeitsperson für die Datenverwaltung innerhalb von 72 Stunden darüber zu unterrichten.
   Dieser entscheidet dann an Hand des Umfanges des Datenverlustes ob die an die Datenschutzbehörde zu melden ist und ob bei hohem Risiko der betroffenen Personen, diese zu unterrichten sind.
   Sollten, durch welche Umstände auch immer, die gesamten Daten der Projektgruppe verloren gehen oder gelöscht werden, so ist auf die Sicherheitskopie aus dem Safe zurückzugreifen.
   Zum Aufbau der gesamten Datenstruktur kann ein entsprechendes Fachunternehmen herangezogen werden.

d. **IT Risiko / Schwachstellenanalyse**
   Sollten Präsentationen der Projektgruppe außer Haus stattfinden, so muss unbedingt darauf geachtet werden nicht den Laptop der Projektgruppe an fremde Techniker zwecks Datenübertragung (Power Point Präsentation) auszuhändigen. Sofern nicht PC‘s der Projektgruppe zur direkten Übertragung genutzt werden können, sind entsprechende USB-Sticks zu verwenden, welche ausschließlich diese Präsentation beinhalten. Es ist darauf zu achten, dass der USB-Stick nach Beendigung der Veranstaltung wieder an den Mitarbeiter der Projektgruppe ausgehändigt wird.

e. **Anpassung der Website an die DSGVO**
   Der Webmaster der Projektgruppe (Kommunikation / Öffentlichkeitsarbeit) ist damit beauftragt, in Zusammenarbeit mit der Projektgruppe, die Website der DSGVO entsprechend anzupassen und zu pflegen.
   Unter anderem die Internetseite auf HTTPS umzustellen und das Impressum entsprechend der Angaben und Nutzung der persönlichen Daten anzupassen.

Breitscheid, den 17.12.2019

XXXXXXXXXXXX
Zuständigkeits-Person
für die Datenverwaltung der Projektgruppe

Bemerkung: Um dem Genderwahnsinn im Text dieses Dokumentes zu entgehen, gelten alle auf Personen bezogenen Aussagen für alle Geschlechter.

Ich habe an der Unterweisung über die Anwendung der DSGVO

am ……..… in……..… teilgenommen.

Ich erkläre hiermit die vorliegenden Anweisungen nach bestem Wissen und Gewissen zu befolgen.

Vorname **Nachnahme** **Unterschrift**