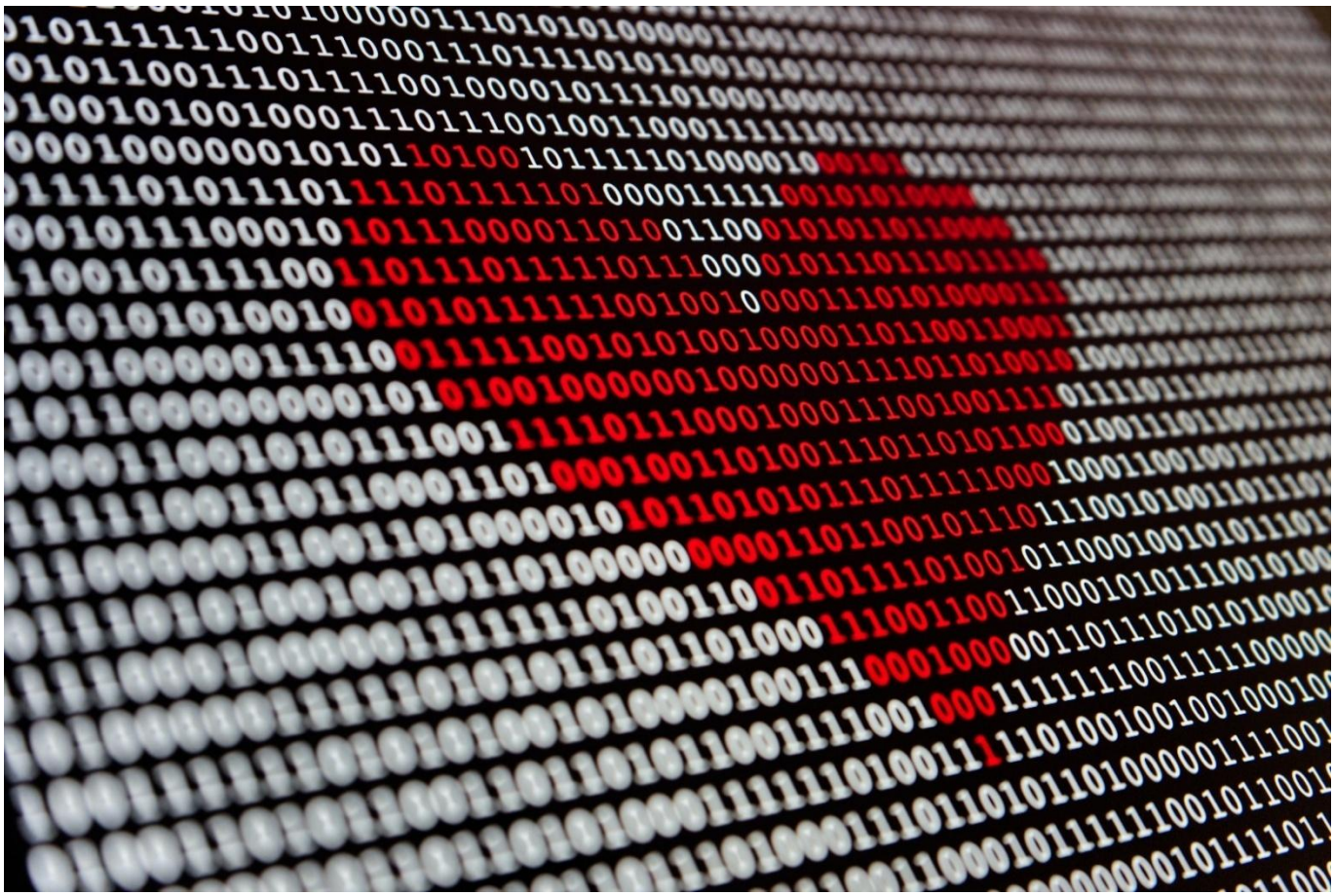
DRK-Generalsekretariat

T41 Digitalisierung & Nachhaltigkeit
Data Science Hub



Datenschutz-Orientierungshilfe für Datenprojekte im DRK

Ein Datenprojekt zu starten heißt, Chancen zu erkennen: die Chance, eure Arbeit zu stärken, vorhandenes Wissen besser zu nutzen oder neue Erkenntnisse sichtbar zu machen. Ob ihr als Haupt- oder Ehrenamtliche gerade beginnt oder bereits Daten sammelt – diese Orientierungshilfe führt euch durch die entscheidenden Schritte eures Vorhabens und unterstützt euch dabei, euer Projekt wirkungsvoll voranzubringen.

Daten verarbeiten bedeutet Verantwortung übernehmen

Wenn ihr in eurem Datenprojekt personenbezogene Daten sammelt oder analysiert, übernehmt ihr eine besondere Verantwortung. Das ist aber kein Grund zur Sorge, sondern eine echte Chance: Projekte, die von Anfang an "datenschutzfreundlich" gedacht sind, schaffen Vertrauen bei ihren Nutzerinnen und Nutzern und sorgen für rechtliche Sicherheit. Ein durchdachter Umgang mit Daten zeigt euren Nutzerinnen und Nutzern, dass ihre Privatsphäre respektiert wird. Diese Orientierungshilfe begleitet euch durch alle Phasen eures Datenprojekts und hilft dabei, die richtigen Fragen zu stellen und gute Entscheidungen zu treffen.

Ab wann braucht ihr eine datenschutzbeauftragte Person?

Nicht jedes DRK-Datenprojekt braucht automatisch eine eigene datenschutzbeauftragte Person. Zur Pflicht wird sie, wenn ihr umfangreich bestimmte Arten von Daten verarbeitet (etwa Gesundheitsdaten) oder wenn Datenverarbeitung zu euren Kerntätigkeiten gehört. Die gute Nachricht: Eine datenschutzbeauftragte Person ist oft schon auf Verbandsebene vorhanden und kann euer Projekt unterstützen. Sie hilft bei der Bewertung von Risiken, berät bei der Auswahl von Rechtsgrundlagen und steht bei Fragen zur Verfügung. Wichtig ist, sie frühzeitig in das Projekt einzubinden - nicht erst, wenn Probleme auftreten. Sie ist eure Verbündete, nicht die Datenschutz-Polizei.

Was ist eine Datenschutz-Folgenabschätzung?

Eine Datenschutz-Folgenabschätzung (DSFA) klingt kompliziert, ist aber im Grunde eine strukturierte Risikoanalyse für euer Projekt. Ihr müsst sie durchführen, wenn eure Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte der betroffenen Personen zur Folge hat. Das kann bei neuen Technologien, umfangreicher Überwachung oder der Verarbeitung sensibler Daten der Fall sein. Die DSFA hilft euch dabei, Risiken frühzeitig zu erkennen und Schutzmaßnahmen zu entwickeln. Sie besteht aus drei Kernfragen: Was macht ihr mit den Daten? Welche Risiken entstehen dadurch? Wie könnt ihr diese Risiken reduzieren? Denkt an die DSFA als Qualitätscheck für euer Projekt - sie macht es besser, nicht komplizierter.

🔗 Umgang mit besonderen Datenkategorien | Stiftung Datenschutz

Mehr dazu später, nun geht es erst mal mit dem Datenprojekt los.

Schnell-Check für den Projektstart

- ✓ Ist euch bewusst, dass ihr mit personenbezogenen Daten besondere Verantwortung übernehmt?
- ✓ Habt ihr geprüft, ob ihr eine datenschutzbeauftragte Person braucht oder bereits jemand auf Verbandsebene verfügbar ist?
- ✓ Wurde beurteilt, ob eine Datenschutz-Folgenabschätzung (DSFA) für euer Projekt erforderlich ist?
- ✓ Habt ihr die datenschutzbeauftragte Person frühzeitig in das Projekt eingebunden?
- ✓ Seht ihr Datenschutz als Erfolgsfaktor für Vertrauen und Qualität, nicht als Hindernis?

Das Projekt vorbereiten & Nutzende informieren

Rechtsgrundlagen verstehen und wählen

Die Datenschutzgrundverordnung (DSGVO) ist ein guter Startpunkt. Sie funktioniert nach einem einfachen Prinzip: Personenbezogene Daten dürfen nur mit einem guten Grund verarbeitet werden. Diesen "guten Grund" nennt man Rechtsgrundlage, und davon gibt es sechs verschiedene. Die bekannteste ist die Einwilligung -

Wichtig dabei:
Personenbezogene Daten dürfen nur auf rechtmäßige Weise und auf eine für die betroffene Person nachvollziehbare Weise verarbeitet werden.

wenn Menschen explizit zustimmen. Aber es gibt auch andere, etwa das "berechtigte Interesse" oder die "Erfüllung einer Aufgabe im öffentlichen Interesse", die für DRK-Projekte manchmal passender sind. Je nach Rechtsgrundlage gelten verschiedene Regeln Rechte für die Betroffenen. Überlegt euch diese Entscheidung gut, denn später ändern ist schwierig. Bei Gesundheitsdaten gelten noch strengere Regeln - hier ist besondere Sorgfalt gefragt.

🔗 Rechtsgrundlagen | Stiftung Datenschutz

Verantwortung klar definieren

Im DRK trägt rechtlich der Vorstand oder die Geschäftsführung die Verantwortung für Datenverarbeitungen in allen Projekten. Das bedeutet: Diese Personen entscheiden, wie Daten verarbeitet werden, und sorgen dafür, dass sich alle an die Regeln halten. Wirksamer Datenschutz entsteht aber nicht von allein - ihr braucht klare Strukturen: Wer darf auf welche Daten zugreifen? Wie werden sie geschützt? Was passiert bei Problemen? Eine Verpflichtungserklärung aller Projektbeteiligten schafft Klarheit im Alltag. Wichtig ist, dass diese nicht nur eine leere Formel ist, sondern konkret erklärt, was in eurem Projekt erlaubt ist und was nicht. So wissen alle Bescheid und können sicher arbeiten.

🔗 Verantwortlichkeit und Haftung im Datenschutz | Stiftung Datenschutz
🔗 Verpflichtungserklärung | Stiftung Datenschutz

Informationspflichten erfüllen

Transparenz ist das A und O des Datenschutzes. Nutzerinnen und Nutzer haben ein Recht darauf zu wissen, was mit ihren Daten passiert. Das bedeutet für euch: Erklärt klar und verständlich, wer ihr seid, welche Daten ihr sammelt und warum ihr das tut. Diese Information müssen vorliegen, bevor ihr die Daten erhebt - nicht erst auf Nachfrage. Eure Datenschutzhinweise sollten wie eine gute Gebrauchsanweisung sein: vollständig, aber nicht überfrachtet, rechtlich korrekt, aber trotzdem verständlich. Denkt daran, dass diese Hinweise Vertrauen schaffen können, wenn sie zeigen, dass ihr verantwortungsvoll mit den Daten umgeht.

Wichtig dabei:
Die Verarbeitung von personenbezogenen Daten muss für die betroffenen Personen nachvollziehbar und verständlich sein. Art, Zweck und Verarbeitung der Daten sollten kommuniziert werden.

🔗 Informationspflichten | Stiftung Datenschutz

Rechte von Betroffenen respektieren

Die DSGVO gibt den Menschen starke Rechte - und das ist gut so. Sie können fragen, welche Daten ihr über sie speichert, falsche Angaben korrigieren lassen oder unter bestimmten Umständen die Löschung verlangen. Für euer Projekt bedeutet das: Ihr braucht klare Abläufe, um solche Anfragen zu bearbeiten. Das Auskunftsrecht ist besonders wichtig - hier müsst ihr nicht nur sagen, ob ihr Daten habt, sondern auch eine vollständige Kopie der Daten herausgeben. Prüft dabei immer die Identität der anfragenden Person, um Missbrauch zu verhindern. Seht diese Rechte nicht als Störung, sondern als Chance: Wer transparent und hilfsbereit mit Anfragen umgeht, stärkt das Vertrauen in sein Projekt.

🔗 Betroffenenrechte nach DSVGO richtig umsetzen | Stiftung Datenschutz

Checkliste für die Projektvorbereitung

- ✓ Ist klar geregelt, wer datenschutzrechtlich verantwortlich ist und wer auf welche Daten zugreifen darf?
- ✓ Habt ihr für alle Datenverarbeitungen die passenden Rechtsgrundlagen ausgewählt und dokumentiert?
- ✓ Werden die betroffenen Personen transparent und verständlich über die Datenverarbeitung informiert?
- ✓ Haben alle Projektbeteiligten Verschwiegenheitserklärungen unterschrieben und wurden geschult?

- ✓ Sind einfache Wege geschaffen, über die Menschen ihre Datenschutzrechte geltend machen können?

Daten beschaffen und Projekt umsetzen

Erfassung von Verarbeitungstätigkeiten

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) ist euer datenschutzrechtlicher Kompass. Es dokumentiert systematisch, was ihr mit welchen Daten macht, warum ihr das tut und wie lange ihr sie behaltet. Stellt euch vor, es ist wie ein Inhaltsverzeichnis für alle Datenverarbeitungen in eurem Projekt. Erstellt das Verzeichnis am besten als übersichtliche Tabelle und arbeitet dabei eng mit allen zusammen, die mit Daten umgehen. So vergesst ihr nichts Wichtiges. Das Verzeichnis müsst ihr jährlich überprüfen und bei Änderungen anpassen. Falls die Aufsichtsbehörde nachfragt, müsst ihr es vorlegen können. Aber das Verzeichnis ist mehr als nur eine Pflichtübung - es hilft euch, den Überblick zu behalten und bessere Entscheidungen zu treffen.

🔗 Erfassung von Verarbeitungstätigkeiten | Stiftung Datenschutz

Verarbeitung von Daten der besonderen Kategorie

Manche Daten sind besonders sensibel - Gesundheitsdaten, Angaben zur Herkunft oder zu politischen Ansichten. Diese "besonderen Kategorien" sind extra geschützt, weil ihr Missbrauch zu Diskriminierung führen kann. Für DRK-Datenprojekte können Daten dieser Kategorie relevant werden. Diese dürft ihr nur in Ausnahmefällen verarbeiten - etwa mit ausdrücklicher Einwilligung. Bei solchen Daten gelten höhere Anforderungen: Ihr müsst zwingend ein VVT führen und bei umfangreicher Verarbeitung eine Datenschutz-Folgenabschätzung machen. Das mag aufwendig erscheinen, aber es spiegelt die besondere Verantwortung wider, die ihr mit diesen sensiblen Informationen übernehmt.

🔗 Umgang mit besonderen Datenkategorien | Stiftung Datenschutz

Mitarbeit von Ehrenamtlichen: Verschwiegenheit gewährleisten

Ehrenamtliche sind das Herzstück vieler DRK-Projekte - auch bei der Datenarbeit. Aber alle, die mit personenbezogenen Daten arbeiten, müssen zur Verschwiegenheit verpflichtet werden, bevor sie anfangen können. Das ist keine Schikane, sondern schützt sowohl die Daten als auch die Ehrenamtlichen selbst. Die Verpflichtungserklärung sollte nicht nur eine trockene Belehrung sein, sondern praktische Hilfe für den Alltag bieten: Wie übertragt ihr Daten sicher? Wer darf was sehen? Was passiert mit den Daten am Ende? Eine praxisnahe und verständliche Schulung schafft für alle Beteiligten Klarheit darüber, was erlaubt ist und was nicht, und lässt sie entspannt an eurem Projekt mitarbeiten.

🔗 Verpflichtungserklärung | Stiftung Datenschutz

Technische und Organisatorische Maßnahmen (TOMs) implementieren

TOMs sind die praktischen Schutzmaßnahmen für eure Daten - von Passwörtern bis zu Backup-Strategien. Die DSGVO schreibt keine konkreten Maßnahmen vor, sondern fordert einen risikobasierten Ansatz: Je sensibler die Daten und je größer das Risiko, desto stärkere Schutzmaßnahmen braucht ihr. Typische TOMs sind Zugangskontrollen, Verschlüsselung, regelmäßige Sicherheitskopien und Schulungen. Aber denkt auch an die Besonderheiten eures Projekts: Arbeitet ihr mit Externen? Nutzt ihr mobile Geräte? Gibt es spezielle Gesetze zu beachten? Plant eure TOMs systematisch und überprüft sie regelmäßig. Sie sind kein einmaliger Aufwand, sondern ein lebendiger Teil eures Projekts, der mitwächst und sich anpasst.

🔗 Technische und organisatorische Maßnahmen | Stiftung Datenschutz

Auftragsverarbeitung und internationale Datenübermittlung

Wenn ihr externe Dienstleister beauftragt - für Cloud-Speicher, Software oder andere Services - verarbeiten diese oft eure Daten mit. Das nennt sich Auftragsverarbeitung und braucht einen detaillierten Vertrag, der genau regelt, was der Dienstleister darf und

was nicht. Der Vertrag muss alle wichtigen Punkte abdecken: Was wird verarbeitet, wie lange, mit welchen Schutzmaßnahmen? Wählt eure Dienstleister sorgfältig aus und prüft, ob sie die nötigen Sicherheitsstandards erfüllen. Besonders knifflig wird es bei internationalen Anbietern: Werden Daten in Länder außerhalb der EU übertragen, braucht ihr zusätzliche Garantien für den Datenschutz. Das können Angemessenheitsbeschlüsse der EU-Kommission oder spezielle Vertragsklauseln sein. Lasst euch hier beraten - internationale Datenübermittlungen sind komplex, aber mit der richtigen Vorbereitung durchaus machbar.

🔗 Auftragsverarbeiter auswählen | Stiftung Datenschutz

Checkliste für die Projektumsetzung

- ✓ Sind angemessene technische und organisatorische Schutzmaßnahmen (TOMs) implementiert?
- ✓ Bei besonderen Datenkategorien: Sind die zusätzlichen Schutzanforderungen erfüllt?
- ✓ Wurden mit allen externen Dienstleistern ordnungsgemäße Auftragsverarbeitungsverträge abgeschlossen?
- ✓ Bei internationalen Datenübermittlungen: Sind die datenschutzrechtlichen Voraussetzungen erfüllt?
- ✓ Werden die Datenschutzmaßnahmen regelmäßig überprüft und bei Bedarf angepasst?

Projektende und Verstetigung

Umgang mit Verletzungen des Datenschutzes

Datenschutzverletzungen passieren - trotz aller Vorsicht. Das kann die falsch adressierte E-Mail sein, ein verlorenes Tablet oder ein Hackerangriff. Wichtig ist nicht, dass nie etwas passiert, sondern dass ihr richtig reagiert. Zuerst: Sofort den Schaden begrenzen - E-Mail zurückrufen, Gerät sperren, Sicherheitslücke schließen. Dann bewerten: Besteht ein Risiko für die betroffenen Personen? Falls ja, habt ihr 72 Stunden Zeit, um die Aufsichtsbehörde zu informieren. Bei hohem Risiko müsst ihr auch die Betroffenen direkt benachrichtigen. Diese kurzen Fristen zeigen, wie wichtig es ist, schon vorher zu wissen, was im Ernstfall zu tun ist. Bereitet euch vor: Wer ist zuständig? Wie erreicht ihr die Aufsichtsbehörde? Welche Informationen braucht ihr? Ein klarer Notfallplan nimmt den Stress aus der Situation.

🔗 Umgang mit Datenschutzverletzungen | Stiftung Datenschutz

Daten aufbewahren und löschen

Am Ende eures Projekts stellt sich die Frage: Was passiert mit den gesammelten Daten? Zwei wichtige Grundsätze helfen bei der Antwort: Zweckbindung bedeutet, dass ihr Daten nur für die ursprünglich geplanten Zwecke nutzen dürft. Ist der Zweck erfüllt, müssen sie weg - außer gesetzliche Aufbewahrungsfristen stehen dem entgegen. Speicherbegrenzung bedeutet, dass ihr schon vor der Datensammlung festlegt, wann ihr sie wieder löscht. Das kann ein festes Datum sein oder an ein Ereignis geknüpft werden. Für die Praxis braucht ihr ein Löschkonzept, dass alle Datenbestände erfasst und klare Verantwortlichkeiten definiert. Wichtig: "Löschen" bedeutet nicht nur "in den Papierkorb verschieben", sondern unwiederbringlich vernichten. Plant das Löschen von Anfang an mit - es ist genauso wichtig wie das Sammeln der Daten.

🔗 Löschfristen und Löschkonzepte | Stiftung Datenschutz

Wichtig dabei:
Personenbezogene Daten dürfen nur dann erhoben werden, wenn es hierfür festgelegte, eindeutige und legitime Zwecke gibt. Die erhobenen Daten dürfen nicht verarbeitet werden, wenn sie mit diesen Zwecken der Erhebung unvereinbar sind.

Checkliste für den Projektabschluss

- ✓ Gibt es einen klaren Notfallplan für den Umgang mit Datenschutzverletzungen?
- ✓ Sind für alle Datenarten klare Speicherfristen definiert und ein Löschkonzept erstellt?
- ✓ Gibt es funktionierende Verfahren für die sichere und vollständige Löschung nicht mehr benötigter Daten?
- ✓ Wurde geprüft, welche Daten noch für welche Zwecke benötigt werden?
- ✓ Sind automatisierte Löschprozesse eingerichtet oder regelmäßige manuelle Löschungen geplant?
- ✓ Wurde dokumentiert, was mit den Daten nach Projektende passiert?
- ✓ Sind alle Beteiligten über die Löschpflichten und -prozesse informiert?

Spezielle Herausforderungen für DRK-Datenprojekte

Besondere Vertrauensstellung und vulnerable Zielgruppen

Das DRK genießt ein besonderes Vertrauen in der Gesellschaft - und das bringt auch besondere Verantwortung mit sich. Viele Menschen, mit denen ihr arbeitet, befinden sich in schwierigen Lebenssituationen und sind besonders schutzbedürftig. Das können Menschen in Notlagen sein, Kinder und Jugendliche, ältere Menschen oder Menschen mit Behinderungen. Diese Personen können oft nicht auf Augenhöhe über die Verwendung ihrer Daten entscheiden. Deshalb müsst ihr noch sorgfältiger abwägen: Ist die Datenverarbeitung wirklich notwendig? Sind die Schutzmaßnahmen ausreichend? Könnt ihr die gleichen Ziele auch mit weniger oder anonymisierten Daten erreichen? Nutzt das Vertrauen, das Menschen in das DRK setzen niemals aus, sondern rechtfertigt es durch besonders verantwortungsvolles Handeln.

Zusammenarbeit zwischen DRK-Ebenen

Das DRK ist föderal organisiert - Bundesverband, Landesverbände, Kreisverbände und Ortsvereine arbeiten zusammen, haben aber oft unterschiedliche rechtliche Strukturen. Für Datenprojekte kann das komplex werden: Wer ist verantwortlich, wenn Daten zwischen verschiedenen Ebenen ausgetauscht werden? Welche Verträge braucht ihr? Wie stellt ihr sicher, dass alle die gleichen Datenschutzstandards haben? Klärt diese Fragen früh im Projekt und dokumentiert sie sauber. Oft ist es sinnvoll, eine federführende Ebene zu bestimmen, die die datenschutzrechtliche Verantwortung übernimmt. Nutzt aber auch die Vorteile der föderalen Struktur: Erfahrungen und Best Practices können zwischen den Ebenen geteilt werden, und lokale Besonderheiten können berücksichtigt werden.

🔗 Weitergabe von Vereinsdaten | Stiftung Datenschutz

Balance zwischen Innovation und Schutz

Als DRK wollen wir innovativ sein und moderne Technologien nutzen, um Menschen besser zu helfen. Gleichzeitig müssen die Daten geschützt werden. Diese Balance zu finden ist nicht immer einfach, aber durchaus möglich. Der Schlüssel liegt in der frühzeitigen Planung: Denkt Datenschutz von Anfang an mit, statt ihn nachträglich "draufzusetzen". Fragt euch bei jeder neuen Technologie: Welche Daten brauchen wir wirklich? Können wir sie pseudonymisieren oder anonymisieren? Welche Risiken entstehen und wie können wir sie minimieren? Oft gibt es kreative Lösungen, die sowohl innovativ als auch datenschutzfreundlich sind. Scheut euch nicht, externe Expertise zu holen - Datenschutz ist ein Fachgebiet, und gute Beratung kann euch viel Zeit und Ärger sparen.

Checkliste für DRK-spezifische Aspekte

- ✓ Wurde die besondere Schutzbedürftigkeit eurer Zielgruppe bei allen Datenschutzmaßnahmen berücksichtigt?
- ✓ Bei Zusammenarbeit zwischen DRK-Ebenen: Ist geklärt, wer datenschutzrechtlich verantwortlich ist?
- ✓ Habt ihr geprüft, ob ihr eure Ziele auch mit weniger oder anonymisierten Daten erreichen könnt?

- ✓ Sind eure Standardeinstellungen so gewählt, dass sie den Datenschutz maximieren?
- ✓ Teilt ihr eure Erfahrungen mit anderen DRK-Gliederungen und nutzt deren Best Practices?

Zusammenfassung: Datenschutz als Erfolgsfaktor

Datenschutz in DRK-Datenprojekten ist kein notwendiges Übel, sondern ein Erfolgsfaktor. Er schafft Vertrauen, reduziert Risiken und kann sogar die Qualität eurer Daten verbessern. Menschen geben bereitwilliger und ehrlichere Informationen, wenn sie wissen, dass verantwortungsvoll damit umgegangen wird. Denkt Datenschutz von Anfang an mit, nicht als Anhängsel. Holt euch Unterstützung, wenn ihr sie braucht - von datenschutzbeauftragten, juristischen Personen oder erfahrenen Kolleginnen und Kollegen. Und vor allem: Verliert nicht den Mut. Datenschutz ist lernbar, und mit der richtigen Herangehensweise wird er zu einem natürlichen Teil eurer Projektarbeit. Die Menschen, denen ihr helft, haben es verdient, dass ihre Daten so sorgfältig behandelt werden wie sie selbst.