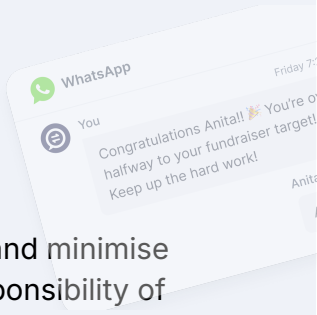
Data Protection Impact Assessment (DPIA) Report for Social Sync



Introduction

A Data Protection Impact Assessment (DPIA) is a process designed to help identify and minimise data protection risks associated with a project or system. Under UK law, it is the responsibility of the data controller—typically the charity or nonprofit organisation utilising the service—to conduct a DPIA when processing activities are likely to result in high risks to individuals' rights and freedoms. Social Sync, as a data processor, assists clients by providing information, compliance documentation, and security policies necessary for effective DPIA completion in accordance with UK General Data Protection Regulation (UK GDPR).

Purpose of the DPIA

This DPIA report assesses potential data protection risks associated with using Social Sync's platform by charities and nonprofit organisations, specifically addressing personal data processing in digital fundraising and stewardship.

---

1. Nature, Scope, Context, and Purposes of Processing

- **Nature of Processing:** Social Sync processes personal data to facilitate digital fundraising campaigns. This includes integrating with platforms like Facebook Fundraising, JustGiving, and GoFundMe to create multi-platform campaigns, as well as delivering personalised stewardship journeys via email, SMS, WhatsApp, Messenger, and Instagram DMs.
- **Scope of Processing:** The platform handles various types of personal data, including supporters' contact information, donation histories, communication preferences, and engagement metrics.
- **Context of Processing:** The processing occurs within the context of fundraising activities conducted by charities and nonprofits, aiming to engage supporters, enhance fundraising efforts, and provide personalised communication.

---

2. Assessment of Necessity and Proportionality

- **Lawful Basis for Processing:** Processing is based on the legitimate interests pursued by the data controllers (charities and nonprofits) in achieving their fundraising objectives. Additionally, explicit consent is obtained for automated communications and special category data processing where required.
- **Data Minimisation:** Only personal data necessary for the specific fundraising and stewardship purposes is collected and processed. The principle of data minimisation is strictly adhered to.

- **Transparency:** Supporters are informed about how their data will be used through clear privacy notices provided by the data controllers.
- **Function Creep Prevention:** Clear data processing agreements with all third-party platforms prevent the use of personal data beyond its original purpose.
- **Data Subject Rights:** Mechanisms are in place to allow supporters to exercise their rights, including access, rectification, erasure, and objection to processing.
- **Safeguarding International Transfers:** Social Sync ensures that any personal data transferred outside the UK and EU is subject to appropriate safeguards, including ICO-approved International Data Transfer Agreements (IDTAs) and Standard Contractual Clauses (SCCs).

---

3. Identification and Assessment of Risks to Individuals

Identified Risk	Description	Likelihood	Severity	Mitigation Measures	Residual Risk
Data Breach Risk	Unauthorised access causing confidentiality breaches and supporter harm.	Medium	High	Robust encryption, secure access controls, regular security audits, and detailed security policy.	Low
Automated Decision-Making Risk	Intrusive automated messaging perception.	Medium	Medium	Explicit consent and straightforward opt-out options.	Low
Third-Party Integration Risk	Security risks from multi-platform data transfers.	Medium	High	Strict processing agreements, GDPR compliance checks for third-party platforms.	Low
Special Category Data Risk	Processing sensitive health-related data.	Low	High	Explicit consent mechanisms, Article 9 GDPR compliance, and data segregation controls.	Low

Data Retention and Control Risk	Excessive data retention reducing user control.	Low	Medium	Clear retention policies and easy user-driven deletion requests.	Low
International Data Transfer Risk	Risks from international data transfers.	Medium	High	ICO-approved IDTAs, SCCs, Schrems II compliance via detailed Transfer Impact Assessments (TIAs), encryption, and ongoing compliance monitoring.	Low

---

4. International Data Transfers and Approved Sub-Processors

Social Sync transfers data internationally under strict ICO-approved mechanisms. Transfer Impact Assessments (TIAs) specifically evaluate risks following Schrems II, ensuring additional supplementary measures like end-to-end encryption, strong key management, and data pseudonymisation are in place. Social Sync commits to continuous monitoring of international privacy laws to maintain GDPR compliance.

Key Measures to Mitigate International Transfer Risks:

- **Use of ICO-Approved Transfer Mechanisms:** Social Sync ensures that all international data transfers are carried out under ICO-approved frameworks, such as International Data Transfer Agreements (IDTAs) or Standard Contractual Clauses (SCCs).
- **Data Encryption and Security:** Data is transmitted using secure channels (e.g., HTTPS with 256-bit encryption) and stored in compliance with internationally recognised security standards, including ISO 27001 and SOC 2 certifications.
- **Vendor Assessments:** Regular risk assessments of third-party service providers are conducted to ensure ongoing compliance with UK GDPR.
- **Minimal Data Transfers:** Personal data transferred outside the UK is limited to the minimum necessary to support fundraising operations, and wherever possible, anonymisation or pseudonymisation is applied.
- **Regular Review:** Social Sync continuously monitors changes in data protection regulations in jurisdictions where personal data is transferred to ensure continued compliance.

Approved Sub-Processors:

Entity Name	Service Description	Country	Security & Compliance Measures
Airtable	Data backups and transfers	US	SOC 1, SOC 2, ISO 27001, IDTA-compliant
Twilio (incl. Sendgrid)	SMS, WhatsApp, Email communications	US	ISO 27001, SOC 2, UK transfer addendum
Loqate	Contact verification	US	ISO 27001, ICO-approved mechanisms
Stripe	Financial transactions processing	US	PCI-DSS compliant
PayPal Giving Fund	Donation processing	US	PayPal Privacy Policy compliance
GoFundMe	Fundraising support	US	GDPR compliance, GoFundMe Privacy Policy
Facebook	Fundraising tools	US	Facebook Privacy Policy
JustGiving	Donation processing	UK	UK GDPR compliance, JustGiving Privacy Policy

---

5. Profiling and Automated Decisions

Social Sync does not conduct profiling or predictive analytics. Automated communications are consent-driven, with clear opt-out options provided.

---

6. Conclusion

By implementing the measures outlined above, Social Sync aims to assist its clients in mitigating data protection risks associated with their fundraising activities. While the responsibility for conducting a DPIA lies with the data controllers, Social Sync is committed to supporting its clients in fulfilling their data protection obligations under the UK GDPR.

Appendix A: Legitimate Interest Assessment (LIA)

Purpose of Processing

Social Sync processes personal data to facilitate charities' and nonprofits' fundraising objectives, enhancing supporter engagement and stewardship through targeted communications.

Necessity of Processing

Processing supporter data is essential to achieving fundraising efficiency and effectiveness, enabling charities to build strong supporter relationships and meet funding targets vital for their charitable purposes.

Balancing Test

- **Benefits:** Significant benefits include improved fundraising outcomes, increased supporter engagement, enhanced stewardship experiences, and strengthened charity-supporter relationships.
- **Impact on Individuals:** Minimal privacy intrusion, as only necessary and proportionate data are processed. Supporters are clearly informed through privacy notices and given control through explicit consent mechanisms and easy opt-outs.
- **Safeguards:** Comprehensive data protection measures, transparency, and robust security standards (e.g., encryption, access controls, regular security audits) ensure minimal risk to individuals.

Outcome

The legitimate interests pursued by the charities and nonprofits outweigh the minimal risks to supporters' privacy rights, provided that all stated safeguards and transparency measures are strictly maintained.