NETLINE BRAND SAFETY CHECKLIST

Navigating the ever-evolving landscape of data compliance and personal information protection is a full-time job. B2B marketers have many questions to answer and can't always be aware of every single thing they need to consider.

For example, here is a quick overview of the risks your business takes without safeguarding your brand:

FINANCIAL RISK

- Fraud
- Fines

REPUTATIONAL RISK

- Content presentation
- User experience

LEGAL RISK

- Privacy
- Terms & Conditions
- Data protection

This is why it's essential to find trusted and informed Vendor Partners that help you protect your clients, employees, and business.

We've created this checklist to simplify the validation process for B2B marketers. This will bring transparency and accountability to the vendor selection process and support you in making the best possible decision for your organization.

COMPLIANCE

CCPA compliance is a black and white issue — vendors either are or are not compliant with the latest data standards and practices. Asking these questions and seeing proof is the only way to guarantee the security of everyone associated with your business.

- □ Is the vendor GDPR compliant?
- □ Is the vendor Privacy Shield Certified?
- □ Can the vendor provide a Certificate of Insurance showing insurance coverage for the follow-
    - □ Commercial general liability?
    - □ Professional liability?
    - □ Cybersecurity?
    - □ Data protection liability?
    - □ Workers' compensation?
    - □ Employers' liability?

DATA PROTECTION and PRIVACY

DATA COLLECTION

Your data represents a significant amount of money for businesses. Regardless of how nicely they ask, not every vendor is up to the task of securing your personal information especially — if they can't answer these questions in the affirmative.

- □ Has the vendor's data collection process been disclosed to you?
- □ Does the vendor encrypt all stored data?
- □ Does the vendor use HTTPS forms?
- □ Does the vendor address the Open Web Application Security Project ("OWASP") Top 10 vulnerabilities?
- □ Does the vendor use SFTP, HTTPS protocols to transfer data?
- □ What are their specified data retention periods?
- □ What method does the vendor employ to securely destroy data after its retention period?
- □ Does the vendor encrypt Pii at rest and in transit?
- □ What infrastructure safeguards are in place to protect systems and applications?

DATA ACCESS

Knowing ***who*** has access to your data is equally as important as knowing ***how*** they get it. Vendors need to have strict policies and procedures in place around how and why specific groups and individuals are permitted to work with personal data.

- □ Does the vendor provide:
  - □ secure logging of activity?
  - □ employee onboarding?
  - □ exit access management?
- □ Does the vendor limit employee access to data based on job function (i.e. on a "need to know" basis)?
- □ Is there a process to inform employees of information security policies and procedures?
- □ Does the vendor have a transparent process to ensure data is safeguarded from unauthorized/inappropriate access and/or loss?
- □ Does the vendor ensure secure access by employees through strong passwords access control?
- □ Does the vendor have written procedures requiring each individual that has access to Personally Identifiable Information to select a strong password (in accordance with applicable industry standards)?
- □ Does the vendor require that each person with access to Personally Identifiable Information change their password at least once every 90 days?
- □ Does your vendor have a written Security Incident Response Policy and a formal Information? Security Incident Response Team (ISIRT)?
- □ Does your vendor perform a background check on all employees that will have access to your data or other confidential data?

TRANSPARENCY

Does your vendor swear to tell the truth, the whole truth, and nothing but the truth? Being confident that a business is worthy of your trust goes a long way.

- □ Can the vendor effectively:
  - □ Articulate why and when a user decided to receive emails from you and/or your clients?
  - □ Show where they've clearly communicated to the user what they will be receiving by opting in?
  - □ Show that subscribers have access to their Privacy Center and/or Preferences center?
  - □ Confirm what those users can expect to receive (i.e.: frequency, format, and content)?
- □ Will the vendor rely on subcontractors or other outside entities to provide all or part of their products? or services?

FRAUD PREVENTION

In B2B marketing, there are many things that, unfortunately, appear too good to be true. Preventing fraud starts with asking tough questions to weed out the pretenders from the real contenders.

- □ Does the vendor host all lead capture forms?
- □ Can the vendor provide call recordings?
- □ Can the vendor show lead authenticity?
- □ Can the vendor show the URL of the website the lead was collected on?
- □ Is the vendor's lead collection form complete?
- □ Does your vendor block click-bots and what is their process to identify and block?

Safeguarding the personal data of your clients, employees, and everyone in between is a great responsibility. The best Vendor Partner for you will be one who is attentive, candid, and (likely) comes highly recommended. Armed with this Brand Safety Checklist, you'll be able to make an informed decision based on trust and your own verification.

Working with NetLine means your business will always be compliant with the latest standards and practices, guaranteeing your lead generation data comes from actively engaged and willing prospects. Start your journey to data compliance today by exploring the NetLine Portal or connecting with one of our platform experts.