

# BLS Email policies

## **BLS Email Acceptable Use Policy**

**Version 1.2**

**Valid from 01/01/2008.**

The B.L.S. Consulting S.r.l. email acceptable use policy (this "**Policy**") applies to B.L.S. Consulting S.r.l. email system ("**BLS**"). Capitalized terms used in this Policy have the meaning set forth in Section 10. This Policy are derived from Habeas Acceptable Use Policy Version 1.1.

### 1. Consent

BLS may only send Email Messages to an individual who has provided Affirmative Consent to receive email from BLS. BLS may obtain Affirmative Consent by one of the two following methods or "Permission Levels":

- a. Confirmed opt-in (a/k/a double opt-in) means an email address collection practice in which, upon being provided clear and conspicuous notice at the point of collection, a purported recipient expressly requests that an email address be included on a list to receive Email, with the following requirement necessary to complete the subscription process: BLS must then send a confirmation email for the purpose of obtaining consent to receive messages selected during the subscription process to the supplied email address, and before mailings commence the recipient must confirm its permission either by taking action at a customer-supplied URI.
- b. Unconfirmed opt-in (a/k/a single opt-in) means an email address collection practice in which, upon being provided clear and conspicuous notice at the point of collection, a purported recipient expressly requests that an email address be included on a list to receive email, but BLS does not take adequate steps before mailings commence to ensure that the email address is valid and capable of receiving email and that the request originated from a source authorized to submit the email address.

Co-registration means an email addresses collection practice in which BLS acquires email addresses by Affirmative Consent through a marketing partner's web site using one of the methods described in Section 1(a) or (b). When acquiring email addresses through co-registration, Habeas Certified Senders, Return Path's Certified Sender or Goodmail Certified Sender are required to perform due diligence in order to ensure that appropriate notice was provided, and relevant consent obtained. Co-registration is an acceptable email address collection practice if and only if BLS acquiring the email addresses is explicitly, clearly, and conspicuously identified at the point of email address collection. Moreover, each act of consent must result in the addition of an email address to only one list. The permission level associated with an address acquired through co-registration is determined by the address collection practice used to acquire such addresses.

Proof of consent, including the date, time, originating IP address, and location (e.g., URL) where the address collection occurred must be produced by BLS upon request.

BLS adhere to the applicable local standards and laws (Italian Privacy Normative D.Lgs 196/2003 and European Commission Privacy and Electronic Communications Directive).

BLS also may send Transactional Email as defined below. A transactional email means an email message the primary purpose of which is:

- c. to facilitate, complete or confirm a commercial transaction that the Recipient has previously agreed to enter;
- d. to provide warranty information, product recall information or safety or security information with respect to a commercial product or service used or purchased by the Recipient;
- e. to provide:
  - i. notification concerning a change in the terms or features of,
  - ii. notification of a change in the Recipient's standing or status with respect to, or
  - iii. at regular periodic intervals, account balance information or other type of account statements with respect to a subscription, membership, account, loan, or comparable commercial relationship involving the ongoing purchase or use by the Recipient of products or services offered by BLS;
- f. to provide information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or
- g. to deliver goods or services, including product updates or upgrades, that the Recipient is entitled to receive under the terms of a transaction that the Recipient has previously agreed to enter.

The definition of "Transactional Email" is intended to mirror the definition of "Transactional or Relationship Message" in the CAN-SPAM Act of 2003 and the regulations promulgated thereunder.

Prohibited Practices.

- h. BLS may not acquire email addresses through list purchase, list rental, list exchange, partner mailings or similar types of email campaigns.
- i. Any form of email prospecting (i.e., where there is no consent or existing business relationship between BLS and the Recipient) by BLS is prohibited.
- j. Email addresses to be used must not be gathered through methods such as scraping, or dictionary harvesting attacks.
- k. Email Addresses must not be sold, shared or exchanged with third parties unless such sale, sharing or exchange is disclosed at the point of address collection.

## 2. Notice

BLS provide clear and conspicuous notice at the point of email address collection about the nature, content, frequency and source of messages which will be sent to the Recipient as a result of completing the subscription process. BLS also provide clear and conspicuous notice at the point of email address collection if the Recipient's email address will be shared, rented or sold causing the Recipient to receive commercial or promotional Email messages from affiliates or third parties.

## 3. Content

BLS ensure that all email messages conform to all applicable laws including, but not limited to, the CAN-SPAM Act of 2003, the Italian Privacy Normative D.Lgs 196/2003 and the European Commission Privacy and Electronic Communications Directive. In addition, BLS comply with the following:

- a. Message headers, subject lines and content shall not be misleading, misrepresentative or falsified in any way.
- b. Messages not transmit viruses or other programs which may destroy or limit the functionality of a computer. Email messages and attachments are verified by two different antivirus software (McAfee Uvscan and Frisk F-Prot), antivirus are updated in 5 minutes from release of new signatures, antivirus engine are update in 10 days from release of new version.
- c. Messages not contain content which is unlawful or harassing.

## 4. Unsubscribe

- a. BLS include an unsubscribe function within each mass mailing message, also instructions for unsubscribe are in disclaimer (direct or link) present in all email messages.
- b. Once an unsubscribe request is received, it be considered permanent and no email messages may be sent to that Recipient unless Affirmative Consent is obtained again. Re-establishment of a business relationship is not sufficient to override a prior unsubscribe request.
- c. BLS unsubscribe a complaining Recipient within 7 calendar days.
- d. BLS acknowledges that in order to process unsubscribe requests and complaints received through the Certified Email program, receiver partners will provide complaint data and email addresses of complaining Recipients to Certify Subject in order for Certify Subject to provide this information to BLS.

## 5. Infrastructure

BLS must maintain an email sending infrastructure that complies with all industry standards and best practices:

- a. The IP address (85.88.193.82, 85.88.193.84, 85.88.193.88) of the reverse DNS entry for the sending email server (mail1.bls.it, mail2.bls.it, dadamail.bls.it) match the IP address of the sending email server.
- b. SPF record version spf1 are defined and maintained for all domains that send email. SPF record are compatible with SENDER ID (ptr not used, ~all instead of -all policy).
- c. All email sends by sending email servers are signed with DKIM signature version 1.
- d. Only email servers of BLS infrastructure are authorized of send emails with BLS domains using port 25, BLS employes and consultant must use port 587 (SASL Authentication, TLS crypted transport) to send emails.
- e. Over 100 of the industry's most widely accessed blacklists for filtering and blocking email are used every day to check IP address of email servers.

- f. Vulnerabilities of email systems are identified every day using Secunia advertising service, patches are applied in 5 days from release date, workarounds are implemented if patches are not released in 15 days from vulnerability disclosure.
- g. List maintenance systems (Dadamail) are employed to reliably receive and process bounces and other notices from receiving networks. BLS adopt and implement a policy for managing addresses that bounce repeatedly (permanent problems immediately removed from list, temporary problems removed from list after 3 unsuccessfully sent each repeated for 1 hour.)

6. Recipient Complaints.

A complaint occurs when BLS receives notice from a Recipient regarding an unwanted email message. BLS will interpret a complaint as a request to unsubscribe and unsubscribe a complaining Recipient in one laborative day.

7. Contact Information.

BLS maintain abuse and postmaster mailboxes for all domains that send email in order to facilitate the receipt and handling of complaints and other issues. BLS maintain accurate contact information in the WHOIS database, and, in addition, BLS provide current and correct contact information in web site.

8. Security.

BLS take reasonable steps to ensure the security of networks used to distribute email and store Recipient information.

- a. BLS ensure that reasonable measures are in place to protect the security and integrity of any Recipients' email addresses held in databases or on electronic systems. Data are maintained only in BLS main site (Via Gramsci 25, 27100 Pavia, Italy) and in Disaster Recovery Site (Via Gramsci 21, 27100 Pavia, Italy). Data are backed up every day.
- b. BLS take reasonable steps to preserve the security of the network sending infrastructure used to distribute email, including the prevention of open proxies, open relays and the dissemination of computer viruses, worms, or trojans on the BLS network and any IP addresses over which email messages are sent.
- c. Recipients' data exchanges are protected by SSL protocol using high secure certificate released by Comodo Certification Authority. BLS holds a website identity assurance warranty of \$500,000. This means that Recipients are insured for up to \$500,000 when relying on the information provided by IdAuthority on this domain.

9. Changes to Policies.

BLS reserves the right to change or modify this Policy at any time. Recipients' will be notified of changes to the terms of this Policy either by e-mail, regular mail or by publication on the web site.

10. Definitions

- a. "***Email Message***" or "***Message***" means any email that is sent by the BLS.
- b. "***Recipient***" means an individual or a business company who receives a Email Message.