

Privacy statement – Red Cross Bumerang Keyring Register

1 Data controller	Finnish Red Cross Tehtaankatu 1 A 00140 Helsinki, Finland Phone: +358 20 701 2000
2 Contact details in matters concerning the register	Finnish Red Cross Tehtaankatu 1 A 00140 Helsinki, Finland Phone: +358 20 701 2000 tietosuoja@redcross.fi
3 Name of register	Finnish Red Cross / Bumerang Keyring Register
4 The purpose of processing personal data	<p>The Keyring Register contains personal data on customers who have registered as users of the Bumerang Keyring Service for the purpose of having lost keys returned to them via the service.</p> <p>The processing of personal data is based on the Bumerang service agreement.</p> <p>The personal data in the customer register is used for the following purposes:</p> <ul style="list-style-type: none"> • customer communications • customer relationship management and development, follow-up offer on the key security service • statistics and monitoring • FRC member and donor marketing • market research or opinion polls <p>Personal data may be processed by third parties for marketing purposes. Third parties may include printing houses or similar cooperation partners that only process data for the purposes of the FRC.</p> <p>Bumerang customer data is stored for three (3) years from the end of the key security service. Payment data is stored for six (6) years in accordance with the Accounting Act.</p>
5 Data content of the register	<p>The following data may be processed in the register:</p> <ul style="list-style-type: none"> • identification data <ul style="list-style-type: none"> ○ names: first name and last name ○ contact details: <ul style="list-style-type: none"> ▪ address: postal code, city, street address ▪ telephone number

	<ul style="list-style-type: none"> ▪ email address <ul style="list-style-type: none"> ○ user language ○ customer number ○ key tag number ○ contact preferences • customer relationship data <ul style="list-style-type: none"> ○ usage history of the key security service ○ product purchases ○ campaign and contact information • data concerning the use of online shop services <ul style="list-style-type: none"> ○ cookie data ○ log data ○ session identifiers ○ IP addresses ○ payment and transaction data.
6 Regular data sources	<p>Customer data is collected for the register in connection with product and service purchases and payment transactions from customers themselves. Personal data is received and updated regularly via Posti's personal data updating service.</p> <p>FRC pages also use cookies, which you can read more about here: www.redcross.fi/cookie-policy/</p>
7 Regular disclosures of data	<p>As a rule, customer register information is not disclosed to third parties.</p> <p>Personal data is only disclosed to the authorities if required by law, for example for the investigation and prevention of misuse.</p>
8 Transfer of data outside the EU or EEA	<p>No personal data is transferred outside the areas of EU Member States or the European Economic Area.</p>
9 Data protection principles of the register	<p>Manual material: Manual material is stored in locked facilities. Access to the work spaces is monitored with access passes.</p> <p>Digital material: Systems containing personal data may only be used by employees whose work role gives them the right to process personal data. Each user has their own user ID and password to the system. Access to the work spaces is monitored with access passes. The data is collected into databases that are secured with firewalls, passwords and other technical means. Databases and their backup copies are located in locked rooms, and the data may only be accessed by specific individuals, named in advance.</p>
10	<p>Data subjects have the right to:</p>

<p>Rights of data subjects</p>	<ul style="list-style-type: none">• request a copy of their personal data• request that their personal data be amended or deleted, unless applicable data security regulations require that the data be retained• request restrictions on the processing of their personal data or oppose this processing• Request that their personal data be transmitted from one system to another, in accordance with applicable data security legislation• refuse, in full or in part, any contact made for the purpose of direct marketing and research• submit a complaint to supervisory authorities. <p>Any requests pertaining to checking or correcting data or the right to refuse contact must be submitted to the controller using the contact details provided in section 2 above.</p>
--------------------------------	--