

MICROCHIP ADVISORY GROUP (MAG) CODE OF PRACTICE FOR DATABASES HOLDING PERMANENT IDENTIFICATION DATA FOR DOGS

General Standards

1. The database operator is to accept and record information regarding owners and animals identified by microchip or other form of permanent identification to the standards set out below.
2. Information is only accepted on the basis of recording the data for the lifetime of the animal.
3. The database operator must accept data from any approved implanter using appropriate microchips or tattooing methods, providing the fee is paid. (An approved implanter is a person trained by or on behalf of a distributor who complies with the BSAVA MAG Code of Practice.)
4. Database operators should not register microchips from distributors that do not comply with the Microchip Advisory Group (MAG) Code of Practice. The MAG Code of Practice is at appendix 2. MAG is a sub-group of the British Small Animals Veterinary Association (BSAVA). Compliance for appendix 2 implementation by April 2006.
5. The cost of recovery of data is at the expense of the database operator and must be built in to the database operator's fees for data recording
6. The database operator must interface, accept or provide information from all other MAG-approved database operators for the purpose of reunification.
7. The database operator must supply information on performance within a reasonable timescale when requested by MAG. A standard report and timescales will be negotiated with MAG.
8. The database operator must comply with the laid down customer service standards as laid down in paragraphs 10, 16-18, 26, 31-33, and 45.

Access to information

9. Database operators must provide a reunification service 24 hours a day, 365 days a year for retrieval of information by authorised persons (e.g. dog wardens, animal welfare organisations, veterinary surgeons and police). Telephone contact must be by means of a single point of contact, implemented via commercial agreement with other database providers and distributors.
10. All database operators must be working towards shared access to owners' contact details to facilitate quicker and more effective reunification. Sharing of information would avoid the need for authorised persons to make several calls before obtaining the information they require.
11. All database operators must keep contact information for other database operators up to date so they can either automatically divert callers to other database operators or provide callers with the relevant telephone numbers.
12. All database operators must have access to other national and international permanent identification databases.
13. Where internet-based services or SMS messaging are provided to both authorised users and to owners, these must comply with the UK security and data protection measures outlined below. Use of internet, web-based and SMS technology must comply with the Privacy and Electronic Communications Regulations 2003 and other relevant current UK legislation.
14. When dealing with re-unification calls a clear record must be taken of where the pet is located. Details of data fields to be collected are given in appendix 1.
15. 90% of all re-unification calls to database operators must be answered within 20 seconds

16. No more than 4% of calls must be lost.

17. Databases must minimise the costs of access to the database and generally the telephone call tariff must be based on national call rate charging.

Confidentiality

18. All database operators must inform the owner at the time of registration (e.g. in writing on registration documents) that their contact details may be released to an authorised third party, such as a dog warden, police officer or animal welfare organisation, in the event of their pet being found.

19. Databases must only give information held on their database to authorised third parties whose PIN number has first been authenticated. Authorisation must be established by first obtaining the full name, address, any relevant job-related code/ID numbers, the name of the organisation, and job title of the individual concerned. The identity of the authorised individual must also be authenticated with their employer. The authorised individual must then be given a personal PIN number or other form of security code so that their identity can be established.

20. Registration information may be used to communicate relevant services, such as pet health insurance, to owners subject to the contractual agreements between the database operator, distributor or manufacturer, and other contracted parties. The initial registration information is not to be sold or passed to a third party other than for the purpose of individual animal retrievals and providing information on database services. All recording and transactions relating to the data should be in strict accordance with the Data Protection Act. It is accepted that, because the relationship between idENTICHIP (the distributor) and Anibase (the database operator) is unique, there will be occasions where idENTICHIP will pass information to a third party for commercial reasons.

21. All data security and control, including data entry or amendment, is the responsibility of the database.

22. An effective and approved multi-level security system must be in use at all times to ensure adequate data protection.

23. Database operators must have procedures in place for the disclosure of information to authorised persons for the purposes of reunification.

Recording of information

24. All details submitted must be on the database operator's own approved forms or other methods approved by the database operator and, where appropriate, signed by the animal owner and verified by use of the implanter's P.I.N. number.

25. Data must be recorded on the database within 5 working days of receipt but the aim should be 2 days.

26. Minimum data fields on the animal, owner and the implanter are specified in Appendix 1 and must be collected and stored on the database.

27. A provision to cross-link owners and animals must be maintained in order to link any owner who has multiple pets or where animals are in joint ownership.

28. Procedures must be in place to ensure that data is only kept for the life-time of the registered animal. This should be achieved by removing records after a specified time period. MAG suggests that, where dogs are concerned, records could be removed and archived 20 years after the date of registration. MAG has decided, based on available evidence, that 11 years is the average life span of a dog and consequently 20 years is a likely maximum.

Updating of information

29. Database operators must make proactive efforts to ensure details held on databases are up to date, using measures such as: the provision of change of address cards with the original registration documents; the provision of an internet updating facility for owners; adverts/editorial in the dog press; reminders to owners. Owners must also be encouraged to provide up to date information.

30. Any updates must be made within 5 working days but the aim should be 2 days.

31. Change in ownership must only be accepted if accompanied by the database operator's official form which is signed and dated by the owner who originally registered the animal. Where the original form is not available the database operator may accept alternative evidence of ownership. Where no evidence is produced a form of relinquishment should be sent to the registered owner before any changes are made.

32. If requested confirmation of any updates and changes must be provided to the owners within seven working days of the change being made to the database.

Accuracy of information

33. Database operators must have procedures in place to ensure the accuracy of information entered and stored on the database.

34. Database operators must have a documented staff training and customer feedback procedure.

35. A multi-level validation process on microchip numbers, telephone numbers, addresses etc must be in use to ensure accuracy.

Information to be provided to owners

36. Full contact details for the database operator -any substantive changes to these details must be communicated to all database users or measures put in place to automatically re-direct telephone calls, faxes, e-mails and postal mail.

37. Telephone numbers – the point of contact for the database operator must be clearly stated.

38. Clear information on the contact details for making administrative queries.

39. Information on how to make updates and any costs involved. Although it is preferable that updates are made free of charge, where a charge is made, costs must be kept to a minimum and wherever possible incentive schemes used such as a once-only payment for unlimited updates.

NB – The Data Protection Act 1998 requires that personal data is accurate and where necessary up-to-date. Therefore if a pet owner provides amendments to their record but refuses to pay, the database operator would be obliged to update the records or cancel membership due to non-payment. DIG would strongly object to any database removing owners' details from their database due to non-payment.

40. Information and advice on the importance of providing change of address details if taking the pet on holiday or if the animal is being looked after temporarily at another address.

41. Information on the importance of informing the database operator of the death of a pet or change of ownership.

42. Data protection statements including advice to the owner that their details will be given to authorised third parties if their pet goes missing.

43. The procedure to follow if a pet goes missing.

44. Confirmation of registration which must be sent within ten working days of receipt of registration information. The owner must also be advised, on the microchip/identification form, to contact the database operator if no confirmation of registration is received within 28 days.

Complaints procedure

45. Database operators must have a reporting mechanism listing failures to link to owner details from the microchip number, and identifying implanters and/or distributors with problems. Adverse reaction reports must be forwarded to MAG.

46. Database operators must have a system for recording and addressing complaints about database activities both from the general public and also from users such as implanters and those accessing the database for data retrieval.

47. Database operators must supply MAG with regular returns outlining nature and scale of complaints received and measures taken to rectify problems. A standard form and procedure will be defined by negotiation with MAG. Such information is commercially sensitive and MAG will ensure it is treated appropriately.

Contingency plans

48. Database operators must maintain an electronic backup of the entire system to enable recovery of all data more than 24 hours old.

49. Database operators must maintain backup communication systems when normal channels fail. This could be achieved by automatic messaging by the exchange.

50. Database operators must at least store monthly electronic backup of the total database in a secure location.

51. Database operators must have agreed procedures in place to protect the availability of data, such as the transfer or sale of data to another approved database operator or transfer to MAG, should the business fail or cease trading for whatever reason. This might be achieved by depositing data in ESCROW together with a full disaster recovery plan.

Service Provider

52. Any person involved in the running of a database (owner, director, operator) should have no criminal conviction or recorded previous breach or contravention of MAG guidelines or Data Protection Act 1998 provisions and will at all times act with the utmost integrity and good faith in all dealings with data received, held and processed and in accordance with all relevant legislation, Codes of Practice and industry guidelines for best practice.

53. The database service provider must have access to proven technical competence in the areas of information storage and distribution and microchip technology.

54. The database operator must have computer hardware and software and procedures adequate to the task.

55. The database operator must comply with all protocols, performance criteria and guidelines prescribed by MAG. Such protocols must be agreed after consultation with database operators and other interested parties.

For information please contact:

BSAVA
Woodrow House
1 Telford Way
Waterwells Business Park
Quedgeley
GL2 2AB

Appendix 1

The following fields of data must be collected at initial registration:

- a. Owner or keeper's full name, address and postcode (*these must all be collected and stored as separate data fields*)
- b. Two contact telephone numbers (e.g. day-time/evening/mobile/work)
- c. pet's name
- d. microchip or tattoo number
- e. collar tag details/number
- f. product
- g. manufacturer
- h. distributor
- i. species
- j. breed
- k. sex
- l. year/date of birth
- m. colour/description/identifying marks
- n. significant medical problems/medication required

The following fields could be collected in order to aid re-unification and welfare of pet until it is returned to its owner:

- a. Owner's e-mail address
- b. 3rd party contact details – nominated by owner
- c. special needs – diet/allergies
- d. contact details for registered veterinary practice
- e. medical problems
- f. vaccination codes
- g. other forms of ID, e.g. tattoo
- h. temporary address e.g. holiday accommodation

The following data must be collected on receipt of a reunification call or report of a lost dog:

Finder

- a. Authorisation code/PIN number of authorised third party
- b. Name and phone number of authorised third party
- c. Name, address and phone number of finder (where the 'finder' is a member of the public and not an authorised third party)
- d. Date and time call was taken
- e. Date, time and place animal was found

Information must be cross-referenced against the database record. All data must be accurate, relevant and not excessive in relation to the purpose for which it is processed.

Owner

- a. Date and time of loss
- b. Location of loss
- c. Current contact details

Appendix 2

CODE OF PRACTICE FOR MICROCHIP DISTRIBUTORS AND MANUFACTURERS

OBJECTIVE

The Code is aimed at producing minimum requirements and standards that should be put in place and adhered to by all microchip distributors, and associated businesses.

The aim is to provide a safe, permanent identification system for companion animals and equines and an effective reunification system for animals that stray.

Adherence to the Code of Conduct is a requirement of membership of the Microchip Advisory Group.

EQUIPMENT

Microchips

Microchips must be supplied in Pre-Packed Sterile (PPS) units which can be either disposable syringe style or re-usable gun formats. All microchips intended for companion animal and equine markets should meet ISO standards 11784 and 11785, the FDXB standard with a 15-MAGit code and pass the performance and competence tests approved by ISO.

The distributor must not supply chips with a country code in the UK until there is a single national authority authorised to issue microchip numbers or with the prefix "999". The PPS unit should be provided in a package, which includes the following:

- Sterilisation indicator
- Expiry date
- Minimum of 3 self-adhesive bar codes advising the unique number for distribution to the owner/keeper, the implanter and the database.
- The delivery container should be batch numbered to ensure full traceability of chips to a particular implanting agent.
- The distributor should have full product liability insurance

It is suggested but not mandatory that

- The supplier offers a microchip that minimises the chance of migration
- The supplier provide a repurchase facility for agents' unused PPS units to ensure their safe disposal

Scanners

Scanners should have passed the ISO approved performance test and be able to read chips that comply with ISO standard 11784 and FDXA chips until 2026. It is suggested that a test chip be included when delivering the Scanner to customers.

Battery powered scanners should have a low battery indicator and stop operating when operating function is compromised by low power input.

The Wide distribution of scanners is an essential element of the microchipping system. The policy of distributors on pricing and availability should reflect their responsibility to maintain the system.

Where a scanner does not fully comply with the ISO standard it must be fully marked as such.

TRAINING

Training should only be carried out by a competent organisation and the quality of the training is the responsibility of the distributor. Training should be specific to the products. Training of implanting agents should be comprehensive and cover:

- a) Introduction
 - Responsible Pet Ownership
 - Health and Safety issues
 - Potential adverse reactions
 -
- b) The Chip
 - RFID technology - how it works
 - ISO 11784 and 11785, other relevant standards
 - Unique numbers, manufacturers' and/or country codes
- c) The Scanner
 - ISO 11785
 - scanning techniques and effect of low battery on performance
 - Effect of environment and interference on the scanners' ability and performance.
 - Performance of individual models of scanners in reading different types of microchip
- d) Implanting
 - Appropriate route of implantation for different types of animals as per RCVS guidance
 - Preparation procedure – preferred implantation sites
 - Migration – local and distant
 - Supervised practice session at implanting animals including restraint
 - Minimum of 2 animals satisfactorily implanted

- e) Databases
 - Purpose: reunification; national and international databases
 - Registration forms/online registration
 - Back track system

- f) Regulations
 - Requirement for collar and tag in dogs and third party liability
 - Pet travel scheme
 - Sharps disposal in accordance with regulations
 - Microchip Adverse Reactions Report Scheme

- g) Insurance
 - Public liability cover essential

A certificate should be issued to non-veterinarian agents along with an Implantation Manual, which confirms the basic contents of the course attended.

Each manufacturer should provide a copy of their Implantation Manual to each transferring Agent.

DATABASE

All Database records held by a manufacturer or supplier or their agents should comply with the Data Protection Act and comply with the MAG database code of practice.

Backtrack System

Each distributor must have a system that enables the registration of the chip number on a reunification database at the point of sale to the implanting agent.

Each manufacturer or supplier must ensure a database maintains the unique numbers of each chip issued and to which implanting agent they have been issued, in order to track stray animals prior to registration on a reunification Database.

Reunification

- a) Databases that are used for reunification directly by finders of strays, e.g. dog wardens and rescue charities, need;
 - A central point of contact and working relationship between national and international databases
 - Data protection procedure. At the time of registration customers should be made aware that the details held on the database about them will be released to a recognised agent, such as a vet, dog warden, police etc; in the event of their pet being found by an agent.
 - The details entered for reunification purposes should be standardised.

- b) Essential details to be taken on owner:
 - Owner/Keeper's full name and address
 - At least 2 contact telephone numbers (day/evening/mobile)

Suggested best practice (additional owner/keeper details)

- Third party contact details
- E-mail address

c) Essential details be taken on owner of Pet:

- Pet's name
- Species
- Breed
- Sex
- Year of birth
- Colour/description
- Chip number and date of registration/implantation

Suggested best practice (additional pet details)

- Pet special needs i.e. diet food
- Vet details
- Medical problems e.g. allergies, diabetes
Medication if applicable

d) A recognised pin number/password should be provided before releasing information to:

- Another database: All the standardised information may be released.
-
- Finder of a lost pet:

- Dog warden, police, veterinary practice, animal charity – owner details disclosed if they give a valid password/pin number.
- General public – should be directed to the appropriate authority e.g. dog warden, veterinary surgeon or police to ensure the microchip is read.

e) Reunification must to be available 24 hours a day and 365 days a year through one telephone number and internet portal..

f) There should be common standards for service levels such as answering calls within a certain time, time scale for entering registration details, etc.

g) Initial registration must be included with the price of the chip and with clear conditions for continued registration and altering the database as owners details change etc.

h) There should be contingency plans to preserve the information on the database and to maintain access to it in case a reunification database suffers a system failure or ceases in business.

POLICING

In the event any distributor becomes aware of the misuse of microchips, for example that microchips are being implanted by untrained Agents or by non-veterinarians in species other than dogs or cats, or other Breaches of the Code of Practice; then

- a. In the first instance it will reported to the chairman of the MAG who will contact the distributor, who will have responsibility to investigate and ensure that there is no misuse or continued misuse

- b. In the event of continued misuse or failure to follow the code of conduct then other sanctions will have to be considered, which may require the intervention of other parties such as Veterinary organisations and ultimately expulsion from the Microchip Advisory Group.

In addition, it is a requirement that the distributors abide by the guidelines laid down regarding microchipping by the RCVS.